



```
105: void WifiScanner::TryLog(Dot11Frame * frm) {
106:     if (is_logging_ &&
107:         logger_ &&
108:         !frm->discard() &&
```



```
105: void WifiScanner::TryLog(Dot11Frame * frm) {
106:     if (is_logging_ &&
107:         logger_ &&
108:         !frm->discard()) &&
```

CONFIDENTIAL AND PROPRIETARY



```
109:     (logger->Write(frm))  
110:     LOG(ERROR) << "Error writing to log";  
111: }
```

```
114:     if (!parser->Parse(frm)) {  
115:         LOG(ERROR) << "Error parsing frame: " << frm->ShortDebugString();
```

















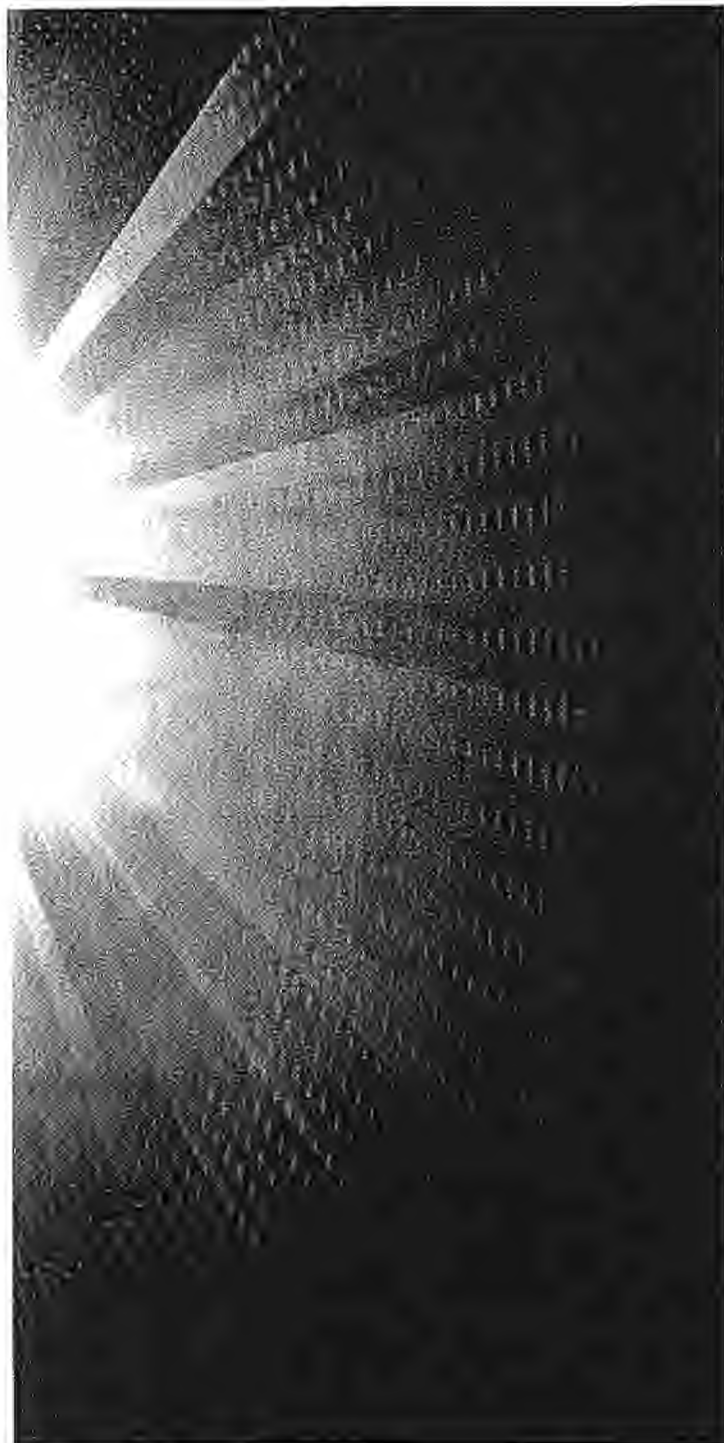








DOCUMENT 11-4



## **Source Code Analysis of gstumbler**

Prepared for Google and Perkins Coie  
Prepared by STROZ FRIEDBERG  
June 3, 2010



## **Table of Contents**

I.	Introduction	1
a.	Executive Summary	2
b.	Basic Technical Descriptions and Definitions	2
c.	Overview of Findings	4
II.	Overview and History of gstumbler, gslite, and Kismet	5
III.	Scope of Review and Methodology	7
IV.	Detailed Analysis and Findings	8
a.	Source Code Flow and Functionality	8
b.	Frame Parsing	10
c.	Default Settings Governing Discard of Data and Writing to Disk	11
d.	GPS Interpolation	12
e.	Command Line Arguments in Configuration Files	13
V.	Conclusion	13
APPENDIX A – Source Code Inventory		14
APPENDIX B – 802.11 Frame Elements		16
APPENDIX C – Protocol Buffer Messages		19

## **I. Introduction**

1. Stroz Friedberg, LLC ("Stroz Friedberg") is a consulting and technical services firm that specializes in digital forensics, data breach and cyber-crime response, on-line and traditional investigations, and electronic discovery. The firm was founded in February 2000 by Edward M. Stroz. For ten years, Mr. Stroz has been a leader in the computer security and digital forensics field, and has pioneered the use of a blend of behavioral science and digital forensics in addressing the insider threat. Before founding what was then Stroz Associates, Mr. Stroz founded and then ran the Computer Crimes Unit of the F.B.I.'s New York office during his sixteen year career with the Bureau. Eric Friedberg, Mr. Stroz's Co-President at Stroz Friedberg, hails from the U.S. Attorney's Office in the Eastern District of New York, where he was the lead cyber-crime prosecutor and the Chief of the Narcotics Unit during his eleven year tenure as an Assistant United States Attorney there. Mr. Friedberg is an expert in cybercrime response, computer forensic investigations, and electronic discovery. Messrs. Stroz and Friedberg, together with the firm's Executive Management, manage the firm's operations. Stroz Friedberg's principal offices are in New York (HQ), Los Angeles, Washington, D.C., London, Dallas, Minneapolis, San Francisco, and Boston. The firm has handled many significant, high-profile digital forensics matters, including a number of source code analyses in the civil, regulatory, and criminal arenas. Mr. Friedberg led the team that conducted the source code analysis in this case.

2. Stroz Friedberg was retained by Perkins Coie, on behalf of Google, to evaluate the source code of an executable deployed on the vehicles otherwise collecting data for Google's Street View service offerings. Specifically, we were asked to provide a third-party assessment of the functionality of the source code for a Google project named "gstumbler" and its main binary executable, "gslite," with particular focus on the elements of wireless network traffic that the code captured, analyzed, parsed, and/or wrote to disk. Stroz Friedberg has no stake in the outcome of this matter and has been asked by Google and Perkins Coie to render a neutral, technical opinion regarding the functionality of gstumbler. Stroz Friedberg is being compensated on a time and materials basis. The project team consisted of three primary examiners/code reviewers and two engagement managers, and our report was internally peer-reviewed by others in the firm.

3. Between May 20 and May 26, 2010, Stroz Friedberg received the gslite source code from Google. The gslite source code is comprised of approximately thirty-two source code files, along with twelve additional files including configuration files, shell scripts, source code repository changelog information, binary executables, and kernel modules. A full inventory of the reviewed source code files and shell scripts is provided in Appendix A. It is our understanding that the provided source code and accompanying shell scripts represent the most current version of the gstumbler application deployed as of May 6, 2010, on vehicles otherwise capturing data for Google Street View. Our findings regarding the application's functionality, based upon our review of the source code, are set forth below: first, in the Executive Summary, and then more specifically in the Overview of Findings and the body of this report.



## **A. Executive Summary**

4. The executable program, *gslite*, works in conjunction with an open source network and packet sniffing program called *Kismet*, which detects and captures wireless network traffic. The program facilitates the mapping of wireless networks. It does so by parsing and storing to a hard drive identifying information about these wireless networks – including but not limited to their component devices' numeric addresses, known as MAC addresses, and the wireless network routers' manufacturer-given or user-given names, known as "service set identifiers," or "SSIDs." The "parsing" involves separating these identifiers into discrete fields. *Gslite* then associates these identifiers with GPS information that the program obtains from a GPS unit operating in the Google Street View vehicle. *Gslite* captures and stores to a hard drive the header information for both encrypted and unencrypted wireless networks.

5. While *gslite* parses the header information from all wireless networks, it does not attempt to parse the body of any wireless data packets. The body of wireless data packets is where user-created content, such as e-mails or file transfers, or evidence of user activity, such as Internet browsing, may be found. While running in memory, *gslite* permanently drops the bodies of all data traffic transmitted over encrypted wireless networks. The *gslite* program does write to a hard drive the bodies of wireless data packets from unencrypted networks. However, it does not attempt to analyze or parse that data.<sup>1</sup>

## **B. Basic Technical Descriptions and Definitions**

6. To understand the functionality of the *gslite* source code, and to understand the Overview of Findings set forth below in Section 1(C), it is important to understand the basic technical concepts critical to the architecture of wireless 802.11 networks and the transmission of data over such wireless networks.

7. Data is transmitted over the Internet via packet switching technology. Briefly, a communication transmitted via the Internet is broken up into "packets" at the point of origination, and the packets of data are routed from the originating device to various other computer devices on the Internet until they reach their final destination. Each packet is comprised of a packet header which contains network administrative information and the addressing information (or "envelope" information) necessary to transmit the data packet from one device to another along the path to its final destination. Each packet also contains a "payload" which is a fragment of the "content" of the communication or data transmission sent and received over the Internet; payload information can include, for example, fragments of requests for URLs, files transferred across the Internet, email bodies, and instant messages, among other things. The packets associated with a particular data transmission may travel over different routes across the Internet to reach their final destination; once they reach the destination device, the packets are reassembled to create the entire transmission.

8. A router is a device on a network that receives a data packet and transmits it to the next router or device on the network. A MAC address is a unique number assigned to a piece of networking hardware, such as a router, by that hardware's manufacturer. Each device and router on a wireless network has a MAC address uniquely identifying that machine.

9. Packets are encapsulated into larger data packages called frames for routing over various network types. Multiple specifications for the transmission of packets using frames have been promulgated by the Institute of Electrical and Electronics Engineers. This report focuses on

---

<sup>1</sup> From an analysis of the source code alone, we cannot ascertain the extent to which *gslite* captures of unencrypted wireless data would be fragmented or complete. Given the factors that the Google Street View vehicles can be moving or stationary and, as discussed below, the *Kismet* device is set to hop rapidly between wireless channels, the numerous wireless data packets that constitute any single user communication may or may not be captured by *Kismet*.

data transmitted over wireless networks pursuant to the 802.11 protocols, the specifications for which provide the international standard for the transmission of data over wireless networks operating in the 2.4, 3.6, and 5 GHz frequency radio bands.

10. There are three primary types of 802.11 frames, which contain information necessary to transmit data packets from one device to another over wireless networks. The three types of 802.11 frames are Control frames, Management frames, and Data frames, each of which is described below:

a. *Control Frames* control access to particular types of networks and facilitate exchanges of Data frames between wireless links. Control frames send the Request to Send (RTS) and Clear to Send (CTS) messages necessary to establish a connection between two links on a network prior to transmitting a data packet (sometimes referred to as a "two-way handshake"). Control frames also transmit the Acknowledgement (ACK) information once a Data frame is received by a link. A diagram of a generic Control frame is provided in Appendix B.1.

b. *Management Frames* contain information necessary to manage a data transmission over the network. Management frames contain, for example, authentication information, information necessary to allocate resources to a transmission, data transmission rates, SSIDs (i.e., network names), information necessary to terminate a connection, and periodic beacon signals. These properties are stored, in part, as Information Elements, that is, id-value pairs in the payload of Management frames. A diagram of a generic Management frame is provided in Appendix B.2.

c. *Data Frames* serve the function of encapsulating and transmitting packets of data over wireless networks. Generally, the body of each Data frame contains the "content" data of the encapsulated packet transmitted over the Internet, including such user-created data as email header information and bodies, URL requests, file transfers, instant messages, or any other communication over the Internet, as well as the addressing information for such transmissions. A diagram of a generic Data frame is provided in Appendix B.3.

d. Each of these frame types have numerous subtypes, which determine, among other things, the fields present in the 802.11 frame. A frame's type and subtype information is stored in the *Frame Control* header field of the 802.11 frame, which is discussed in more detail below.

11. At a high level, an 802.11 frame can be considered to have two distinct sections: the header data and the body data. The header data is comprised of the Frame Control, duration or id, MAC addresses, sequence control number, and quality of service, or QoS, control information. The body data is comprised of the frame body component of an 802.11 frame, to the extent the frame's type and subtype calls for this field. As noted, the body of a Data frame may contain packet content data.

12. A diagram of a generic 802.11 frame showing its various components is below:

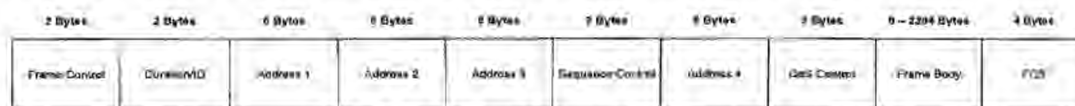


Figure 1, Generic 802.11 Frame Format.

The Frame Control, Duration/ID, Address, Sequence Control, and QoS control fields are considered the 802.11 *frame header*, while the frame body contains the payload data previously discussed. The FCS field contains checksum information used to confirm that the wireless frame was accurately received.

13. Every 802.11 frame contains a 16 bit Frame Control field that contains information regarding the status of the frame and the wireless transmitter of the frame. Specifically, the Frame Control field contains the following properties: Protocol Version; Type; Subtype; To DS; From DS; More Fragments; Retry; Power Management; More Data; Protected Frame; and Order. The Type field is a two bit field that will be 00, 01, or 10 to indicate if a frame is a Management, Control, or Data frame respectively, and the Subtype is a four bit field used to specify the frame's subtype. The To DS and From DS fields are single bit values that specify the routing of the 802.11 frame across the wireless network.

14. The Protected Frame bit in the Frame Control field is also known as the frame's "encryption flag." The Protected Frame field is a single bit which identifies whether the wireless network's transmissions are encrypted; it has no relation to the payload within any Data frame or whether that encapsulated packet transmission is itself independently encrypted. For example, if a fragment of a secure, encrypted HTTP session (HTTPS) were encapsulated in the payload of a Data frame on an unencrypted wireless network, the Data frame's encryption flag would still be set to "0", i.e. "false", indicating that the frame is unencrypted. The 802.11w-2009 amendment to the 802.11 specification, which was approved on September 11, 2009, provides a mechanism to also encrypt unicast Robust Management frames, which will result in the Protected Frame field being set to "1", i.e. "true."

15. Each 802.11 frame type contains at least one MAC address associated with the wireless local area network (LAN). 802.11 frames can contain up to four such MAC addresses associated with a particular wireless LAN.

16. Each wireless network has a public name, known as the SSID. The SSID name may be set by the owner of the wireless network. The SSID can be publicly broadcast to all wireless devices within its range. The broadcast feature also can be disabled so that the SSID for a particular wireless network is not readily visible to devices seeking wireless networks even though the SSID is still ascertainable from the transmitted packets.

17. The 802.11 wireless specifications divide each of the frequency bands into *channels*, analogous to TV channels. The division is regulated by individual countries, resulting in different locales having different numbers of permitted channels in each band. For example, in European countries, the frequency bands are regulated such that transmission is permitted across thirteen overlapping channels between 2.4 and 2.4835 GHz, each of which is 5 MHz apart and 22 MHz in width. A particular communication is transmitted over only one channel; thus, to the extent a packet sniffer is set to "hop" through channels—similar to changing a radio or TV channel—it may only collect fragments of a particular communication.

### **C. Overview of Findings**

18. Using the more technical terminology in the above section, we expand on our high-level findings.

19. As set forth above, the executable program, *gslite*, is an 802.11 wireless frame parsing and collection tool that associates GPS coordinates with wireless network frames. While running in memory, the program parses frame header information, such as frame type, MAC addresses, and other network administrative data from each of the captured frames. The parsing separates the information into discrete fields for easier analysis. In addition, per-packet information regarding the wireless transmission's strength and quality is captured and associated with each frame. All available MAC addresses contained in a frame are also parsed. All of this parsed header information is written to disk for frames transmitted over both encrypted and unencrypted wireless networks.

20. The gslite program discards the frame bodies of 802.11 Data frames sent over encrypted wireless networks. The program inspects the encryption flag contained in each frame header to determine whether the frame is encrypted, i.e., whether it is being transmitted over an encrypted wireless network. If the encryption flag identifies the wireless frame as encrypted, the payload of the frame is cleared from memory and permanently discarded. If the frame's encryption flag identifies the frame as not encrypted, the payload—which exists in memory in a non-structured bit stream of ones and zeros—is written to disk in a serialized format, as further described below.

21. The gslite program parses Management frame bodies and stores the parsed data as "Information Elements." The gslite program also parses Control frames' subtype information before writing it to disk. By contrast, gslite does not parse Data frames' bodies, which may contain user-created content. Rather, unencrypted Data frames' bodies pass through memory unparsed and are written to disk in their unparsed format. (Again, encrypted frame bodies are dropped entirely.)

22. As set forth above, the gslite source code includes logic that examines wireless frames' type and encryption status, and determines whether to discard them in whole or in part. The default behavior of gslite is to record all wireless frame data, with the exception of the bodies of encrypted 802.11 Data frames. The gstumbler application is configurable through the use of command line arguments that make it possible to specify, at the time the program is run, what types of wireless frames to record. Based on our review of the provided configuration files and shell scripts used to launch gslite, prior to May 6, 2010, the gstumbler application used the default configurations described above, which is to say that all wireless frame data was recorded except for the bodies of 802.11 Data frames from encrypted networks.<sup>2</sup>

## **II. Overview and History of gstumbler, gslite, and Kismet**

23. The source code reviewed is from a project referred to at Google as "gstumbler." According to internal Google documentation, gstumbler was first created and used in 2006. At that time, the program executable was itself also named "gstumbler," but at some point in or after late 2006, the executable deployed to vehicles otherwise capturing data for Google's Street View services was revised and renamed "gslite." The gslite program is the focus of this source code review. In this report, "gslite" refers to the specific executable program for which Stroz Friedberg reviewed the source code; and "gstumbler" refers to the overall application, including the configuration files and shell scripts that the Google Wifi project has used to detect and collect wireless network data.

24. The gslite source code is written in C++. C++ is an object oriented programming language, where objects are defined as data structures comprised of properties and methods, i.e. values and functions. An "object" refers to an instance of a data structure in memory. The gslite program makes use of object oriented programming to represent 802.11 frames in memory, parsing the raw frame data and storing its structural elements in a Dot11Frame object as defined in the source code file packet.proto. The Dot11Frame object is defined using a framework called Protocol Buffers, which was developed at Google to provide a means for writing complex data structures to disk. Protocol Buffers are discussed more fully in Appendix C.

25. The gslite program parses some, though not all, information from 802.11 wireless frames read in from a source of wireless frames. It simultaneously receives geolocation coordinates from a GPS system and then associates each wireless frame with the time and approximate location in which it was received. The gslite program works in concert with a second program, Kismet, which must run simultaneously. Kismet controls one or more wireless cards on a Google vehicle

---

<sup>2</sup> It is our understanding that on May 6, 2010, in response to regulatory attention, the gstumbler shell script was revised to disable all Data frame capture. We have inspected that revised shell script and have confirmed that revision.

and provides gslite with the stream of detected wireless frames. The relationship between gslite and Kismet is depicted in Figure 2.

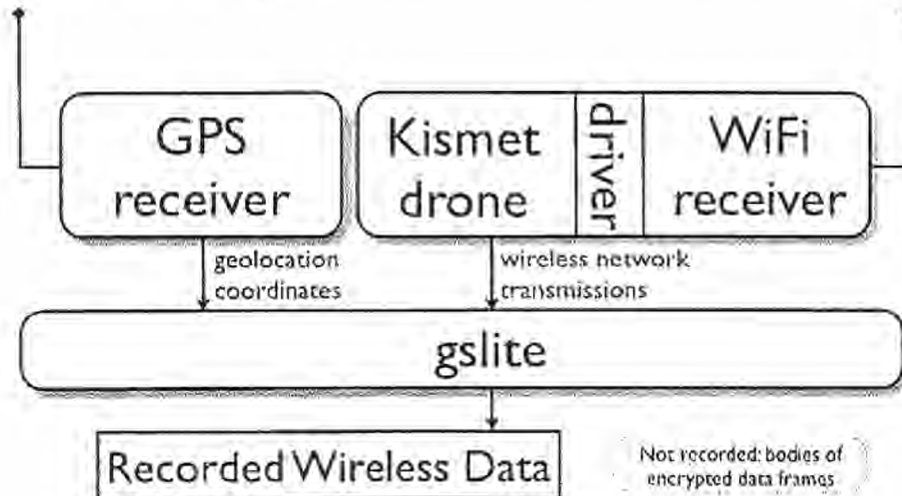


Figure 2. Inputs to gslite.

26. Kismet is a freely available, open-source application for wireless network detection and packet sniffing. Kismet captures wireless frames using wireless network interface cards set to monitoring mode. The use of monitoring mode means that Kismet directs the wireless hardware to listen for and process all wireless traffic regardless of its intended destination. Kismet captures wireless frames passively, meaning that Kismet receives such transmissions without actively transmitting to nearby wireless networks. Kismet only detects packets passively. Through the use of passive packet sniffing, Kismet can also detect the existence of networks with non-broadcast SSIDs, and will capture, parse, and record data from such networks.

27. Kismet is a standalone application capable of capturing and filtering wireless frames. However, it can also be deployed in a configuration called a “drone,” which does not record or analyze network traffic but instead forwards captured traffic to a server listening for such traffic. The Kismet drone program places a Kismet header describing the properties of the wireless transmission in front of the raw 802.11 frame and passes it to gslite for further processing. The gslite application listens for data from a Kismet drone running simultaneously within the Street View vehicle.

28. A Kismet drone is configured through the use of a file named `kismet_drone.config`, which provides, among other things, instructions for Kismet to “channel hop.” Channel hopping is the act of cycling through numerous 802.11 channels per second in order to capture frames from as many nearby networks as possible. In the `gstumbler` project, Kismet’s configuration file is created using a predefined template file, and entries in Google’s template instruct the drone to change wireless channels five times per second, as shown below (`kismet_drone.conf.template` lines 37-41):

```
# Do we channelhop?
channelhop=true

# How many channels per second to we hop? (1-10)
channelvelocity=5
```



As discussed above, the number of permitted channels for broadcast in a given frequency is regulated by a country's local authorities, and the number of permitted channels for broadcast in a frequency ranges between 11 and 14. The `kismet_drone.conf.template` file directs which channels should be monitored and the order through which they are hopped. In the United States, for example, there are 11 channels that may be used to wirelessly transmit data within the 2.4 GHz band. Accordingly, when configured for the United States, Kismet listens to each of the 11 channels for one fifth of a second, thus listening to every channel for one 0.2 second interval during each 2.2 second channel hopping cycle.

### **III. Scope of Review and Methodology**

29. Upon receipt of the `gslite` source code, Stroz Friedberg conducted a high-level review of the `gslite` framework code and associated modules. The purpose was to understand the basic logic flow and functionality of the program, and the significance and dependencies of the various components.

30. Based on our high level review, Stroz Friedberg identified key modules and dependencies for closer scrutiny, and assessed the significance of Google commands and code modules called from libraries external to the `gslite` code for use within the program. We received confirmation that particular functions and modules were borrowed from standard, shared libraries within Google. Because we also confirmed that such functions and codes were not customized for use in `gslite`, but were merely imported to perform standard functions, we focused on the core functionality and key programming modules unique to `gslite`.

31. We also did not independently review the Kismet program. As noted above, 802.11 frames initially are captured by the Kismet program, an open source packet sniffing program. It is our understanding based upon representations from Google that Kismet source code was not modified or adapted in any way as part of the `gstumbler` project.

32. We compared 802.11 frame specifications to the `gslite` frame parsing parameters encoded into the program to verify that the code's parameters are consistent with the specifications. That is, if the code parses particular bits of frame header information to determine, for example, the type of frame or whether the wireless network is encrypted, we confirmed that the program looks at the correct frame bits to parse the expected field from the raw data.

33. We closely scrutinized the parsing functionality of the `gslite` program as it pertains to each type of 802.11 frame. We determined how different types of frames are parsed, the different fields parsed for each frame type, what 802.11 frame fields are written to disk in parsed formats versus raw formats, and what 802.11 fields are discarded and not written to disk.

34. We analyzed the overall structure of code to determine the program's default behavior and the ways in which default behavior may be changed by command line arguments. We also examined the command line configuration settings over the course of `gslite`'s deployment.

35. We confirmed our understanding as to other secondary functions of the program, including its logic to detect bad frames and not process them, its diagnostic capabilities for assessing proper functioning of the program, its calculation and correlation of GPS geolocation information with detected wireless networks, and its decision as to how and when to write data to disk.

36. Stroz Friedberg did not receive or analyze earlier versions of the `gslite` source code or its predecessors. We did, however, review the modification history and did not observe significant changes to the program regarding how frames are parsed and recorded. We also reviewed all available versions of the shell scripts used to launch Kismet and `gslite` to verify what command line arguments were used.

#### IV. Detailed Analysis and Findings

##### A. Source Code Flow and Functionality

37. At the highest level of description, Google's `gstumbler` program creates a series of servers and objects that interface with the Google Street View vehicle's GPS system and the Kismet drone, pulls wireless frames from a stream provided by the Kismet drone, and then assigns timestamp and geolocation information to each wireless frame it encounters, saving the results to disk. The general description of how `gstumbler` operates is illustrated in Figure 3, below, and in the following paragraphs.

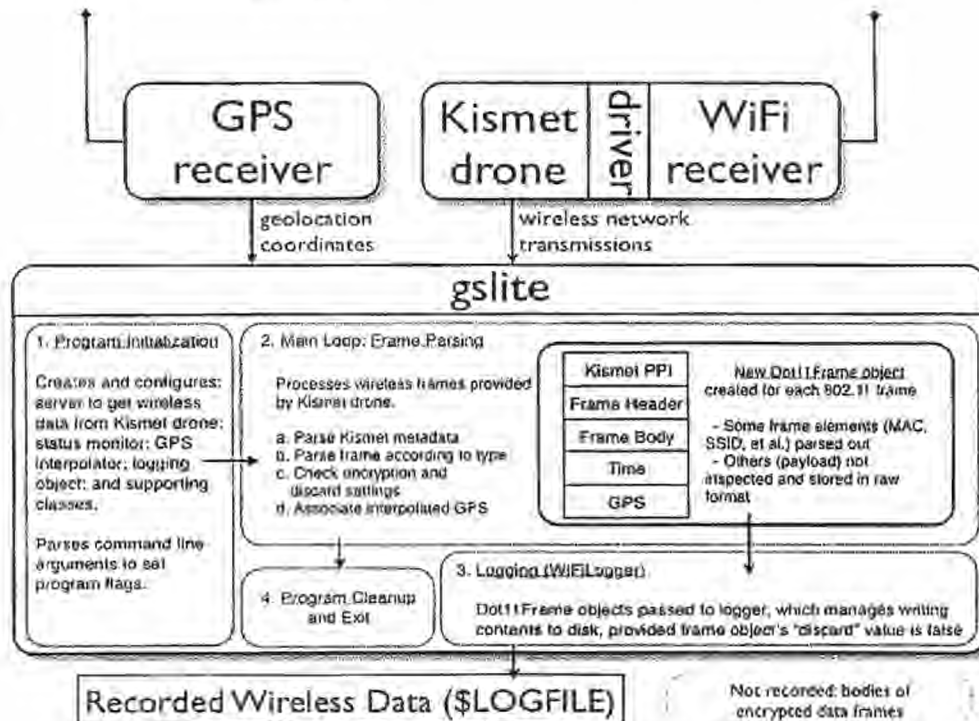


Figure 3: High-level representation of `gslite` program execution

38. The program first parses any command line arguments passed to it from the shell script, `run_gstumbler`, used to launch `gslite`. The program starts and configures a series of services, including, but not limited to: a `WifiRecordLogger`, which manages the storing of 802.11 frame data to disk; and a `WifiLiteServer` object, which listens for Kismet data on a predefined port.

39. For each frame being processed, the program creates a new `Dot11Frame` object in which to store the parsed 802.11 frame fields, along with a pointer to it. The `Dot11Frame` is a data structure that is built using Google's Protocol Buffers libraries. As noted previously, information about `Dot11Frame` objects and Protocol Buffers in general is provided in Appendix C.

40. The program parses the per-packet information (PPI) header information Kismet affixes to a captured 802.11 frame. PPI includes the quality of the signal, the signal strength, the signal noise, if the capture source indicated there was an error in the capture to Kismet, transmission channel, the signal carrier, the signal encoding, and the data transmission rate. The program

also sets the Dot11Frame's time received, time sent, and raw data properties to match those of the corresponding incoming frame.

41. The program proceeds to parse the 802.11 frame as described more fully in section B, below. The gslite program runs the Parse() method of a number of PacketParser objects against the incoming 802.11 frames: Dot11ParserImpl::Parse(); CtrlParserImpl::Parse(); MgmtParserImpl::Parse(); and TruncateParserImpl::Parse(). Although the forms of information available in a given frame vary according to its type and subtype, the packet parsers are applied to all frames regardless of type. The parsing process populates numerous properties of the Dot11Frame object with information extracted from the 802.11 frame. Parsing does not include inspection of the bodies of Data frames.

42. During the TruncateParserImpl::Parse() parsing function, gslite reads the encryption flag on each frame. That bit is located within the second byte of the Frame Control on an 802.11 frame. If the encryption flag is set to "true," then the frame's body, or payload, is cleared from memory and permanently discarded. If it is "false" the frame's body is retained for writing to disk.

43. The GPS interpolator associates geolocation coordinates with the frame and writes the coordinates into the Position property of the Dot11Frame.

44. The parsed 802.11 frame object is written to disk using WriteProtocolMessage() method of the RecordWriter object. In the case of Management frames, the body is written to disk as parsed Information Elements, while in the case of unencrypted Data frames, the body is written to disk in unparsed format. It is our understanding based upon representations from Google that the RecordIO module, used to write the Dot11Frame objects to disk, is a common shared library within Google, and it is utilized unchanged in gslite.

45. The main loop of the program continues parsing, collecting, and geolocating each 802.11 frame as it is detected and forwarded by the Kismet drone. An interrupt signal sent from a user or from the operating system will cause the program to exit the main loop, clean up objects in memory, and exit.

46. The gslite program also writes logging information, largely regarding program status and error conditions, to a default system location. Our review found one line of code that, when executed, writes the content of a wireless frame to disk, through the use of a protocol buffer method for formatting a data structure as a string (scanner.cc lines 114-115):

```
if (!parser->Parse(frm)) {  
    LOG(ERROR) << "Error parsing frame: " << frm->ShortDebugString();
```

The second line of code above writes the wireless frame to disk, including its body, regardless of frame type or encryption flag. However, the program only performs this logging when a wireless frame cannot be successfully parsed and the Parse() method returns false. Our review of the Parse() method determined that this condition is met only when a frame's length is too short to constitute a valid frame header. In such an event, the frame also would be too short to contain a frame body. Furthermore, any such invalid frame would be discarded by Kismet or the wireless card prior to being forwarded to gslite. Accordingly, the circumstances necessary to invoke this logging action preclude the possibility that frame payload content would be written to the error log.

47. During execution, gslite also reports certain diagnostic information in HTML format to the HTTP server to provide in-vehicle feedback regarding the status and operating state of gslite. This status monitor does not write output to disk.

48. Finally, we note that the gslite source code contains functions and methods that are never executed, and which appear to constitute vestigial or uncalled code. Stroz Friedberg



inspected such code but found no control flow that would lead to the execution of such code areas.

## **B. Frame Parsing**

49. Following capture of the data by Kismet, gslite uses a Dot11Frame object to represent the structure of an 802.11 frame in memory, prior to writing the frame to disk. The gslite program processes these Kismet packets by removing the Kismet header, and then processing the underlying raw data, which is an 802.11 frame.

50. "Parsing" a property of an 802.11 frame results in its value being assigned to a property of Dot11Frame object, making it readily accessible for further analysis by gslite without additional decoding. Some 802.11 frame fields are analyzed by gslite and never assigned to a specific property of the Dot11Frame field object. Only some 802.11 frame fields are assigned to properties of Dot11Frame objects in their parsed form by gslite prior to being written to disk; others are stored in memory in a property field named "raw" and are written to disk without being further processed. By default, in the case of encrypted 802.11 Data frames, the frame's body, which was temporarily stored in the Dot11Frame's raw field, is cleared from memory and never written to disk.

51. Specifically, gslite parses all available 802.11 frame header information and stores those properties in memory in a Dot11MacHeader object. The remaining frame data, the body, is stored in its raw form in the raw property field of a Dot11FrameBody object. A Dot11MacHeader object is a representation of the 802.11 frame header in the memory of a computer. Similarly, a Dot11FrameBody is a representation of the body or payload of an 802.11 frame body.

52. The Dot11MacHeader's properties and the Dot11FrameBody object may be further analyzed or parsed depending on the type of frame. Dot11FrameBody objects contain ManagementFrameBody and ControlFrameBody objects to represent metadata specific to Management and Control frames respectively:

- a. Control frames undergo the least additional analysis as they contain comparatively less data than other frame types. Only the subtype information from an 802.11 Control frame's Frame Control field will be parsed and stored in memory as its own parsed property.
- b. Management frames, which contain the administrative information necessary to manage wireless transmissions, undergo both additional analysis, and parsing. Management frames' Frame Control properties are analyzed to determine the values of the To DS and From DS fields, which indicate the number of MAC addresses within the frame; however, these values are not stored in their own property fields in memory. Furthermore, Management frames' bodies are parsed and stored as a series of Information Elements in the ManagementFrameBody's collection of InformationElement objects. Included in the Information Elements properties is the SSID. The gslite program parses and stores the SSID information for all wireless networks, whether the SSID is broadcast or not. Any extra data stored in the ManagementFrameBody is stored in the "extra" property. Once this process is complete, the raw property of the Dot11FrameBody object is then cleared for Management Frames.

53. Although Data frame header information is further analyzed during the parsing process, Data frame bodies are not parsed. Specifically, gslite analyzes a Data frame's Frame Control field to determine the values of the To DS and From DS fields contained therein; however, these values are not parsed or stored in their own properties in memory.

54. In summary, the parsing function of the gslite program does the following:

- a. All 802.11 frames have all of their available 802.11 frame header information parsed and stored in properties of a Dot11MacHeader object in memory, regardless of frame type. A frame's body will be stored as raw data in a Dot11FrameBody's raw property, and this raw data may be further parsed if the frame is a Management Frame. The frame type information from a frame's Frame Control field is parsed and stored in memory as its own value, regardless of frame type.
- b. If the frame is a Control frame, the subtype information from the Frame Control field will be parsed and stored in memory as its own value. No additional parsing is performed on Control frames.
- c. If the frame is a Management frame, the To DS and From DS fields from the Frame Control field are analyzed, but are not parsed and stored in memory as their own properties. Management frame bodies are parsed and stored as a series of Information Elements in ManagementFrameBody's collection of InformationElement objects (which is in the Dot11Frame's Dot11FrameBody object). Any extra data in the body is stored in the ManagementFrameBody's "extra" property, and the "raw" property of the Dot11FrameBody object is cleared.
- d. If the frame is a Data frame, the To DS and From DS fields from the Frame Control field are analyzed, but are not parsed and stored in memory as their own properties. Data frame bodies are not parsed. As discussed more fully below, the body of a Data frame is discarded if the Protected Frame bit is set to "true", which indicates the frame is encrypted; otherwise, the body is written as unparsed data to disk.

### **C. Default Settings Governing Discard of Data and Writing to Disk**

55. After gslite's program logic parses each 802.11 frame according to its type, a Dot11Frame object exists with all available frame properties parsed and stored in the appropriate property fields. At this point in the execution of the program, the program's settings are checked to determine whether or not to retain the current frame data in whole or in part.

56. By default, gslite records all wireless frame data, except for the bodies of Data frames from encrypted wireless networks. The code governing whether data elements of a frame should be retained or discarded occurs in the file "packetparserimpl.cc." Four variables, or flags, are assigned default Boolean values to establish the program's default behavior regarding what to discard from memory and what to retain. In particular, the default settings, as shown below, are set to discard the bodies of encrypted frames<sup>3</sup> and to retain everything else (packetparserimpl.cc lines 14-21):

```
DEFINE_bool(discard_encrypted_body, true,
    "Discard bodies of encrypted 802.11 frames");
DEFINE_bool(discard_control_frame, false,
    "Discard 802.11 control frames");
DEFINE_bool(discard_data_frame, false,
    "Discard all 802.11 data frames");
DEFINE_bool(discard_management_frame, false,
    "Discard all 802.11 management frames");
```

<sup>3</sup>Although a Management frame of the subtype Authentication would have its encryption flag set to "true," the sequence of the execution path causes such Management frame bodies to be stored in the "extra" property and written to disk. Management frames do not contain user content.

57. The same file, `packetparserimpl.cc`, contains the code that checks each wireless frame processed and determines whether or not to retain it in whole or in part, based upon the Boolean values of the flags defined above. The program checks to see whether the "discard\_encrypted\_body" flag is set to "true", which is the default setting. If so, `gslite` checks the frame being parsed to see whether its encryption flag is set to "true." If both checks return "true" then the frame is encrypted and the program discards the encrypted frame's body. The frame body is cleared, using the accessor method `clear_body()`.

```
if (FLAGS_discard_encrypted_body && PacketUtil::IsEncrypted(f)) {
    // Discard just the body of encrypted frames
    f->clear_body();
}
```

Subsequently, when the remainder of the frame is written to disk, its body is not recorded.

58. The program checks the type of the frame being parsed (that is, whether it is a Control, Data, or Management frame) and then checks the value of the corresponding Boolean flag from among the discard flags above. If it is "true", the discard flag of the current frame object is set using the `Dot11Frame` accessor method `set_discard(true)`.

```
switch (PacketUtil::Type(f)) {
case Dot11FrameBody::CONTROL:
    if (FLAGS_discard_control_frame)
        f->set_discard(true);
    break;
case Dot11FrameBody::DATA:
    if (FLAGS_discard_data_frame)
        f->set_discard(true);
    break;
case Dot11FrameBody::MANAGEMENT:
    if (FLAGS_discard_management_frame)
        f->set_discard(true);
    break;
default:
    break;
}
```

59. At a subsequent point in program execution when a parsed frame is to be written to disk, the discard flag of the frame object is checked; if the flag is set to "true", the frame is not written to disk (`scanner.cc` lines 105-111):

```
void WifiScanner::TryLog(Dot11Frame * frm) {
    if (is_logging_ &&
        logger_ &&
        !frm->discard() &&
        !logger_>Write(frm))
        LOG(ERROR) << "Error writing to log";
}
```

#### **D. GPS Interpolation**

60. The onboard GPS system provides geolocation coordinates at some rate slower than the rate at which wireless frames can be received. Accordingly, `gslite` interpolates the position at which each wireless frame was received and associates the interpolated position with the frame object. Stroz Friedberg's review of source code relating to GPS coordinate interpolation found no code execution paths that would affect the wireless data written to disk by `gslite`.

### ***E. Command Line Arguments in Configuration Files***

61. The Boolean flag definitions set forth in section C above provide the default program behavior. However, the flags can be superseded by command line arguments defined in accordance with Google's coding standards. The first line of code executed by gslite processes any and all command line arguments (see gslite.cc lines 12 and 128-129, below). It is our understanding from Google that InitGoogle(), a method defined outside the scope of the provided source code, sets the values of program variables using the command line arguments. The Google standards for using command line flags is documented at <http://google-gflags.googlecode.com/svn/trunk/doc/gflags.html>.

```
#include "base/commandlineflags.h"
...
int main(int argc, char** argv) {
    InitGoogle(argv[0], &argc, &argv, true);
```

62. Command line arguments will supersede the default values for the discard and encryption flags discussed above and change the behavior of gslite. Since the flag "discard\_data\_frame" is false by default, gslite will discard entire Data frames if and only if the flag "discard\_data\_frame" is run on the command line at the time of program execution (or until such time as the default behavior is revised in source code).

### **V. Conclusion**

63. Gslite is an executable program that captures, parses, and writes to disk 802.11 wireless frame data. In particular, it parses all frame header data and associates it with its GPS coordinates for easy storage and use in mapping network locations. The program does not analyze or parse the body of Data frames, which contain user content. The data in the Data frame body passes through memory and is written to disk in unparsed format if the frame is sent over an unencrypted wireless network, and is discarded if the frame is sent over an encrypted network.

## APPENDIX A

### INVENTORY OF REVIEWED SOURCE CODE FILES AND SHELL SCRIPTS

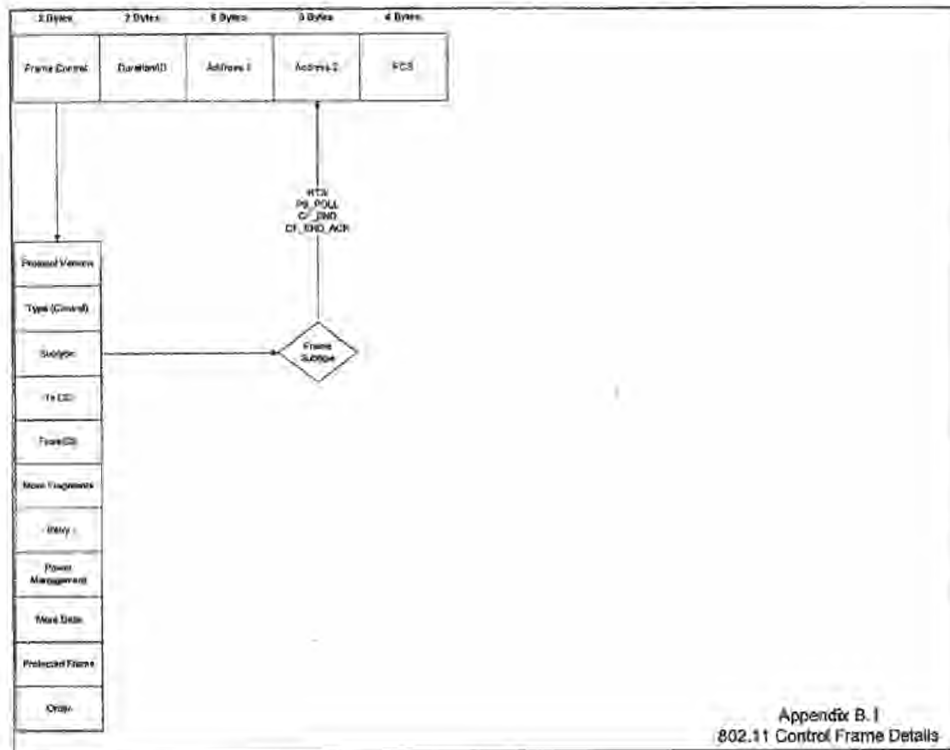
Stroz Friedberg reviewed the following provided C++ source code, configuration files, and shell scripts as part of its static source code analysis. The dates of last modification are derived from the compressed tar files in which the source code was provided and are believed to correspond to the dates of modification of official, checked-in source code.

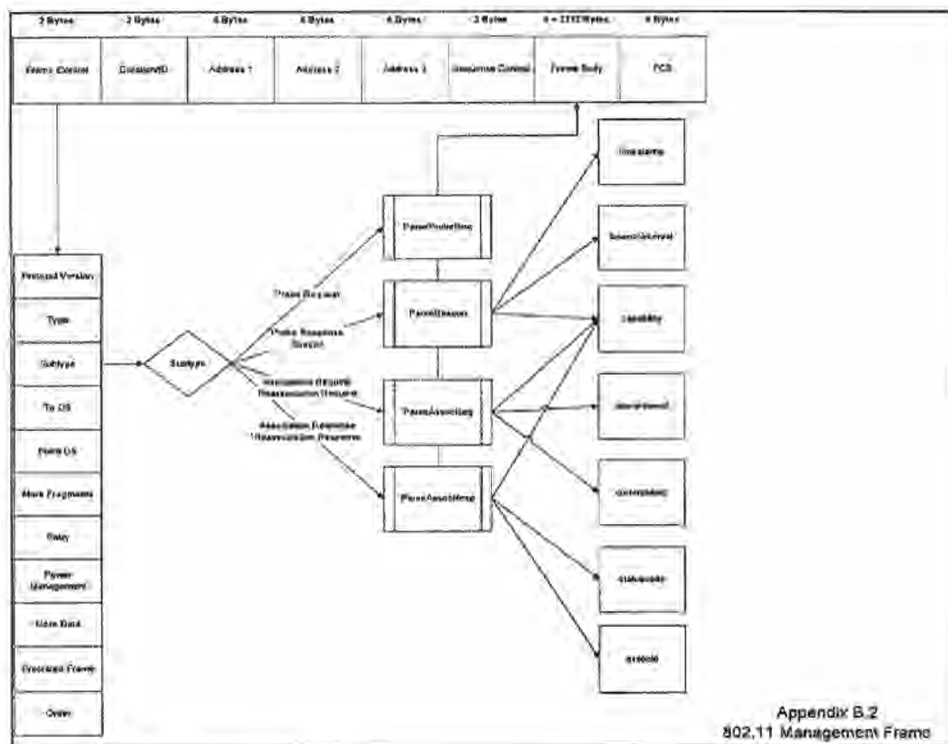
File Name	Last Written On	SHA-1 Hash Value
<b>gstumbler Source Code</b>		
Provided as gstumbler-src.tgz on 5/20/2010		
BUILD	7/1/2009	7de19d35307cfdc91c8c03c9d8d44aee3cebcbaa
gps_messages.h	3/31/2010	aa9ce1443f3e1352056751cdc3ca8d35705cbf1f
gps-interpolator.cc	11/7/2007	37001680b7e4acd0410fd890523fa911371cdf63
gps-interpolator.h	4/30/2008	688d310771e86e2ecc92c7069059bda2e378d1d8
gps-interpolator_test.cc	2/2/2010	21e241b6c0b0ae6512d395f38d5541d0e12b3ed8
gps-ipc.cc	3/31/2010	2413c0538add2323321a25ba1498274f54e2d76f
gps-ipc.h	3/31/2010	175183adb5116594e6f644c9b9bb8a9920476d8a
gps-ipc_test.cc	3/31/2010	3ea76455f6fd12391c6e60ad9d8b0fe9bfb0db4
gslite.cc	3/31/2010	796c67b420fd5f0afbc65c42c07d08256886d3
gstumbler.cc	4/30/2008	2104989f9c44b9c53acbf5bc6857ee8f1fc2594e
gstumbler-run.sh	3/5/2007	e5045fac3b9e6de3ce36b3b797e504a9c741254a
kismetconnection.cc	8/19/2009	4b3cb2d4ef03c53bdf3f46088039c1105d29f63
kismetconnection.h	8/19/2009	cacbb8ca54136cc1bcf3a64f9a54a25b4939f2a7f
logger.cc	11/7/2007	03f2733398191d36fae6297564b455086bdfda83
logger.h	11/7/2007	83d12f13e50f5e070af8f4acf1c032ca6a2f8682
monitor.cc	10/31/2006	7b5381eb9adeb12e09589f84e817f1170bc783ade
monitor.h	10/31/2006	84870c0f3df0b169ef352b0c3f920bd48f6073c
packet_proto	3/31/2010	872e43bb2477b3d50dfdd34f68adad7290f49f6c
packetparser.cc	10/31/2006	f42667c8f5be1580ce46476eb840e0022280d969
packetparser.h	7/1/2009	3855b17808778d752824ea6a2efbe875307933ac
packetparser_test.cc	2/2/2010	dc795a3e99ec890db87d1e97ac835ed3f74a3f7b
packetparserimpl.cc	10/31/2006	ec094b96ab14ba7bf251160ad6d3285d4fa3a714
packetparserimpl.h	10/31/2006	d8f5c40b3954133c8be46e6cabf9f23f91de6ecc
packetsource.cc	10/31/2006	ble6dec9aa9d4a4095c0ad34c9f103b7344154d5
packetsource.h	3/4/2010	69f2b4ffa32e925e56bdf0f56097cf5bd7ce0ed9
packetsourceimpl.cc	12/16/2009	75828b368c1682ebac547c1193e9d3fbc27f54a
packetsourceimpl.h	7/1/2009	bff09f7f55cdd080eaf1d9057a8a33c1d9cbb8f8
packetutil.h	1/28/2008	8dedee1c5b43811bd7a16ea9b5afc58b69adf212
resources/drive_status.tpl	10/18/2007	065c489ee01d5de2f185f92829fceebed58359e9
scanner.cc	3/31/2010	33d4a92a87a679faf0932e492f1be6cf32a9534a
scanner.h	3/31/2010	4a869a3f54a4f2662c09b8fd90e4e14bf631cb83
scanner_test.cc	2/2/2010	7a8004d0c19cc1337ca9cb888bd3f7830a26413b
<b>Configuration files and shell scripts -- most recent versions</b>		
Provided as gstumbler-config.tgz on 5/20/2010		
config_interfaces.sh	5/18/2010	51c00340e9744dda850ca0ee546bccc067327caa
kismet_drone.conf.template	5/18/2010	f5bd93b3fc1ba8ada0827cc04fc6ca5c24aab99c

run_gstumbler.template	5/18/2010	7b3aacb15f8b878b8bd91d34242c8b4a1e958691
run_kismet	5/18/2010	7c8b2b13061b6cb8290256556910d56b93848a20
<b>Configuration files and shell scripts -- historical versions</b>		
<b>Provided as gstumbler-scripts2.tgz on 5/26/2010</b>		
config_interfaces.sh#1	5/26/2010	7b85ea7c7babd7a7115f0caa1fc1e3a2814f9d75
config_interfaces.sh#2	5/26/2010	faeeebfae425597af82acebdc2cc2c972088b10
config_interfaces.sh#3	5/26/2010	5816de44b2c167116958e7bd35240bf113186953
config_interfaces.sh#4	5/26/2010	fc5ee14d002970d532ec55cee09962959b78d28b
run_gstumbler.template#1	5/26/2010	9a718b8727a2c590e670fc08ea271a4818309253
run_gstumbler.template#2	5/26/2010	4l4ca3f5d2175eecd1fc104e8aba702cce34778
run_kismet#1	5/26/2010	27df00844852cd7e0070d82324ab5cc2fb81881c
<b>Supporting library for managing record writing</b>		
<b>Provided as bulkstorage.tgz on 5/26/2010</b>		
bulkstorageblock.h	11/1/2006	d7240f808766bd718e80f1293dcaba95ff50af18
bulkstoragewriter.cc	3/12/2007	e361e6c9d16cc64a115bb3df6a6cdd58e049b61
bulkstoragewriter.h	3/12/2007	d0dad03725314183a9107c7ea004c8d8e26f78d1
bulkstoragewritermanaged.cc	3/4/2010	bab20ee94c25d62c2d8a18259915bf0906d68115
bulkstoragewritermanaged.h	3/4/2010	1d8b671468f0b3d7dbe4f609548261b37fed4eb0
disk_write_methods.cc	3/12/2007	134aea15d93f667e322e7c70c7b89609755e2052
disk_write_methods.h	12/29/2006	4609dcf39b55cc2e111f338b7dbc4a3caf891109
performancemonitor.cc	8/10/2007	f4aece5bd4bcbdd520e654ab0d9802c560c2efc09
performancemonitor.h	11/29/2006	b8c37eb8a427fdd72f707985661a71641c7436ac
sectensecminstats.cc	11/29/2006	34d884b123216a4fb5bd640bf51d2e8f2ad42ef1
sectensecminstats.h	6/22/2009	38c8bf84879ecdade44a31642b5aba0e30e6cccd

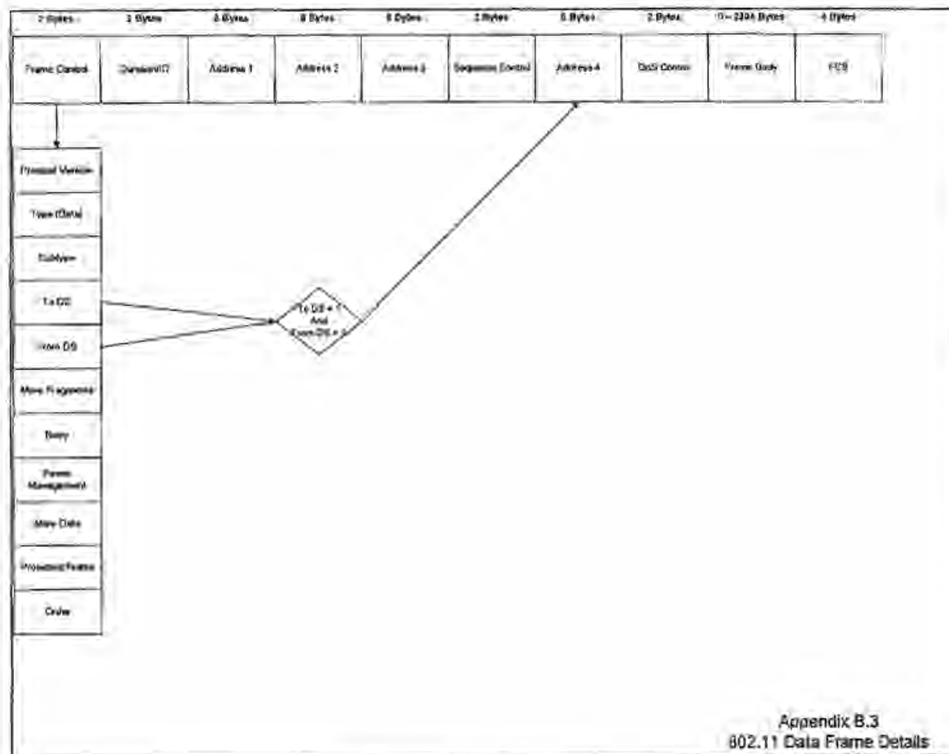
## APPENDIX B

### 802.11 FRAME ELEMENTS









## APPENDIX C

### THE GSTUMBLER DOT11FRAME PROTOCOL BUFFER AND SUMMARY OF RECORDED CONTENT

C-1. Google source code employs a serialization format, accomplished through the use of objects developed at Google called Protocol Buffers, which are used to exchange and write structured data. Protocol Buffers take an object representing a complex data structure and transform that structured object into a bitstream, suitable for transmission or writing to disk, through a transformation called serialization. The source code for protocol buffers was released under an open source license by Google in 2008. An overview of documentation regarding protocol buffers is available at (<http://code.google.com/apis/protocolbuffers/docs/overview.html>).

C-2. Each type of object to be serialized is specified as a Protocol Buffer "message," which establishes the structure of each object type. In the gstumbler project source code, Protocol Buffers are declared in the file packet.proto. The protocol buffer message of central importance to gslite's functionality is the Dot11Frame object, a message that is a structured representation of a single 802.11 wireless frame. The Dot11Frame object contains multiple other protocol buffer messages, also defined in packet.proto, that represent various components and types of wireless frames.

C-3. Protocol buffers provide accessor functions to set and retrieve the values of fielded data within a message. Standard accessor functions include get\_<fieldname>, set\_<fieldname>, and clear\_<fieldname>, where <fieldname> is one of the defined data elements within the message. As discussed in paragraphs 57 and 58 of this report, the Dot11Frame accessor methods clear\_body() and set\_discard(true) will be called if certain flags and conditions are true. These methods serve, respectively, to clear only the content of the Dot11Frame's Body field and to set the Discard Boolean flag of a Dot11Frame message to true. These two methods are the means by which a frame is written to disk without its payload or not at all.

C-4. The following tables summarize the properties within each of the protocol buffer messages defined in packet.proto.

Dot11Frame Object	
Property	Description
Raw	A buffer used to store the unprocessed data; this buffer contains the raw frame data parsed throughout frame processing and is cleared prior to the data being written to disk.
Header	A Dot11MacHeader object in the protocol buffer message format described below.
Body	A Dot11FrameBody object in the protocol buffer message format described below.
Position	A cityblock.PositionInfo object containing GPS coordinates.
PositionComment	An optional string.
TimeRecvd	The time the frame arrived for processing.
TimeSent	The estimated time the frame was transmitted.
KisMetadata	A KismetMetadata object, described below, containing per-packet information including 802.11 channel, signal quality, and frame length.
Discard	A boolean flag that indicates whether or not the entire frame – metadata and body – should be written to disk.

Dot11MacHeader	
Property	Description
Raw	The raw data buffer containing the data that is processed and stored in the header's fields.
FrameControl	A thirty-two bit integer used to store the sixteen bit Frame Control field in an 802.11 frame.
DurationOrId	A thirty-two bit integer used to store the sixteen bit field in position bytes 2 to 3 in an 802.11 frame. These sixteen bits are either the duration or id depending on the type and subtype of the frame.
Address1	The first Media Access Control (MAC) address in an 802.11 frame. A MAC address is a six byte hexadecimal address specifying a network device.
Address2	The second MAC address in an 802.11 frame.
Address3	The third MAC address in an 802.11 frame.
SequenceControl	The sixteen bit sequence control number present in data and management frames. Data may be fragmented for transmission or re-transmission. If the data is fragmented, this number is used to determine where in sequence a fragment fits. This field is zero for the first or only fragment of data, and incremented for each successive fragment sent.
Address4	The fourth MAC address in an 802.11 frame.
QoSControl	Sixteen bits of quality of service related information and policies sent by hardware supporting quality of service.

Dot11FrameBody	
Property	Description
Raw	The raw data buffer containing the data that is processed and stored in the body's fields.
FrameType	An enumerated type that specifies if a frame is: a Management frame (0); a Control frame (1); a Data frame (2); a Reserved type frame (3); or if there is no frame type detected (9999).
Ctrl	An optional ControlFrameBody object, defined below.
Mgmt	An optional ManagementFrameBody object, defined below.

ControlFrameBody	
Property	Description
Subtype	An enumerated type specifying the subtype of a Control frame. Its potential values are: PS_POLL (10); RTS (11); CTS (12); ACK (13); CF_END (14); CF_END_ACK (15); and NO_CTRL_SUBTYPE (9999).

ManagementFrameBody	
Property	Description
Subtype	An enumerated type specifying the subtype of a Management frame. Its potential values are: ASSOC_REQ (0); ASSOC_RESP (1); REASSOC_REQ (2); REASSOC_RESP (3); PROBE_REQ (4); PROBE_RESP (5); BEACON (8); ATIM (9); DISASSOC (10); AUTH (11); DEAUTH (12); and NO_MGMT_SUBTYPE (9999).
AuthAlgorithm	A thirty-two bit integer that is not set in the code reviewed.
AuthTransaction	A thirty-two bit integer that is not set in the code reviewed.
BeaconInterval	A thirty-two bit integer that is used to store the sixteen bit value of the number of time units between target beacon transmission times.
Capability	A thirty-two bit integer that is used to store the sixteen bit series of flags outlining the functionality of the transmitter.

CurrentBSSID	A sixty-four bit integer that is used to store the forty-eight bit MAC address of the access point with which the transmitter is currently associated with.
ListenInterval	A thirty-two bit integer used to store the sixteen bit value of how often a receiver in power saver mode wakes to listen to Beacon management frames.
ReasonCode	A thirty-two bit integer that is not set in the code reviewed.
AssocID	A thirty-two bit integer that is used to store the sixteen bit value assigned by an access point during the association process.
StatusCode	A thirty-two bit integer that is used to store the value used in a response management frame to indicate the success or failure of a requested operation.
Timestamp	A sixty-four bit integer used to store the value of the timing synchronization function timer of a frame's source.
IEs	A collection of Information Elements, or key-value pairs regarding a transmitter.
SSID	A string containing the name of the access point.
Channel	A thirty-two bit integer used to store the channel on which a frame was sent.

KismetMetadata	
Property	Description
hdrlen	A thirty-two bit integer used to store the length of the Kismet header.
drone_ver	A thirty-two bit integer used to store the sixteen bit value of the version of the Kismet drone.
datalen	A thirty-two bit integer used to store the length of the data captured by Kismet.
caplen	A thirty-two bit integer used to store the length of the data originally captured by Kismet.
tv_sec	A sixty-four bit integer storing a timestamp in seconds.
tv_usec	A sixty-four bit integer storing a timestamp in microseconds.
quality	A thirty-two bit integer used to store the sixteen bit value signal quality.
signal	A thirty-two bit integer used to store the sixteen bit value signal strength.
noise	A thirty-two bit integer used to store the sixteen bit value signal noise level.
error	A thirty-two bit integer used to store the eight bit value whether the capture source told Kismet the frame was bad.
channel	A thirty-two bit integer used to store the eight bit value of the hardware channel that received the frame.
carrier	A thirty-two bit integer used to store the eight bit value of the signal carrier.
encoding	A thirty-two bit integer used to store the eight bit value of the signal encoding.
datarate	A thirty-two bit integer used to store the value of the data rate, which is in units of 100 kbps.
adapter	A thirty-two bit integer used to store the mapped value of an adapter name.



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

December 10, 2010

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
236 Massachusetts Avenue, N.E., Suite 110  
Washington, DC 20002

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of Google's responses ("Responses") to the November 3, 2010, letter to Google from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission (the "Bureau Letter") in the above-referenced matter.

As shown below, portions of the Responses to each of the numbered requests in the Bureau Letter contain information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential,"<sup>1</sup> and Exemption 7(C), which provides a statutory basis for withholding from public inspection information compiled for law enforcement purposes and that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."<sup>2</sup> We enclose herewith both a complete, unredacted copy of the Responses, to be treated as confidential, and a separate copy of the Responses marking specific portions thereof as Redacted.

Response No. 2. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection and the

---

<sup>1</sup> 5 U.S.C. § 552(b)(4). *See also* 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

<sup>2</sup> 5 U.S.C. § 552(b)(7)(C). *See also* 47 C.F.R. 0.457(g)(3).



company's internal review and actions taken in response to the matters that have evolved. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. See 47 C.F.R. § 0.459(a)(4).

Response No. 3. The redacted portion of the Response contains sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. See 47 C.F.R. § 0.459(a)(4).

Response No. 4. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company's internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Further, the Response includes trade secrets such as descriptions of the processes by which Google creates and produces such products as Google Maps and Google's related geolocation server, which is highly confidential and competitively sensitive information. Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. See 47 C.F.R. § 0.459(a)(4).

Response No. 5. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, the company's internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Further, the Response includes trade secrets such as descriptions of the processes by which Google creates and produces such products as Google Maps and Google's related geolocation server, which is highly confidential and competitively sensitive information. Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly

competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

Response No. 6. The redacted portion of the Response contains sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

Response No. 7. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection and the company's internal review and procedures taken in response to the matters that have evolved. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

Response No. 8. The redacted portion of the Response contains sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company's internal review and actions, including its internal regulatory compliance procedures and actions. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

Response No. 9. *See* Response No. 11, below.

Response No. 10. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. The information includes Google's internal decisional processes "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Further, the Response includes trade secrets such as descriptions of the processes by which Google creates and produces products, which is highly confidential and competitively sensitive information. Google does not routinely



disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. See 47 C.F.R. § 0.459(a)(4).

Response No. 11. Documents 11-1, 11-2, 11-3, and 11-5 are confidential and proprietary documents that contain sensitive and detailed information regarding Google's private business and internal operational actions and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Further, the Documents contain trade secrets, including product design and computer code, which is highly confidential and competitively sensitive information. Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to business and operations of Google. See 47 C.F.R. § 0.459(a)(4).

The redacted portions of the Responses also are entitled to confidential treatment because their disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy," 5 U.S.C. § 552(b)(7)(C). As the Third Circuit has explained, the purpose of FOIA Exemption 7(C) is to "provid[e] broad protection to entities involved in law enforcement investigations in order to encourage cooperation with federal regulators," and "[c]orporations ... involved in law enforcement investigations ... face public embarrassment, harassment, and stigma because of that involvement." *AT&T Inc. v. FCC*, 582 F.3d 490, 498 n.5 (3<sup>rd</sup> Cir. 2009), *cert. granted*, *FCC v. AT&T Inc.*, No. 09-1279, 177 L. Ed. 2d 1151; 2010 U.S. LEXIS 5745; 79 U.S.L.W. 3193 (September 28, 2010). As Google has explained publicly, it deeply regrets the events that led to the inadvertent collection of Wi-Fi data, and it has been called to answer for its actions in both legal proceedings and the public media. Google respects that the Commission has a law enforcement role in these matters, and it is Google's intention to cooperate fully with this investigation, including explanations of how the incidents occurred, the management review and actions involved, and the security steps taken.

Google has not made the information redacted in the Responses available to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and state attorneys general. Google believes it is necessary for the Commission to maintain the confidentiality of this information throughout the investigation and thereafter until it is destroyed.

**Lampert, O'Connor & Johnston, P.C.**

December 10, 2010

Page 5

Consistent with 47 C.F.R. § 0.459(d)(1), Google respectfully requests notification by the Commission if release of the redacted material in the Response is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "E. Ashton Johnston", with a long horizontal flourish extending to the right.

E. Ashton Johnston  
Mark J. O'Connor  
*Counsel to Google Inc.*

Enclosures

cc: Hillary DeNigro, Chief, Investigations and Hearings Division, Enforcement Bureau  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau



**RESPONSES OF GOOGLE INC. TO LETTER OF INQUIRY  
FILE NO. EB-10-IH-4055**

**I. PRELIMINARY INFORMATION AND GENERAL OBJECTIONS**

**Request for Confidential Treatment.**

Enclosed herewith is Google's Request for Confidential Treatment of Google's responses covered by Exemptions 4 and 7(C) of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential" and "records or information ... that ... could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. §§ 552(b)(4) & (7)(C). *See also* 47 C.F.R. § 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

In addition, Google responds to the Letter with the expectation and understanding that, consistent with Bureau practices and applicable law, details of the Bureau's investigation will not be made public by any Commission employee.

**General Objections.**

Google objects to each question below to the extent it calls for the production of documents and information protected by the attorney-client privilege or the work product doctrine. Google is not producing such documents or information at this time. As explained below in response to Request No. 11, Google has not undertaken a comprehensive review of email or other communications at this time and requests forbearance in the preparation of a privilege log.

Google objects to each question below that assumes or calls for a legal conclusion as to whether communications were "intercepted." To the extent any of the following Requests include a reference to the term "intercept" or "interception," Google's response is without regard to the legal meaning of the term, does not constitute an admission that any communications were intercepted as a matter of law, and this objection applies.

**II. SPECIFIC RESPONSES TO REQUESTS FOR DOCUMENTS AND INFORMATION**

The following responses are made subject to and without waiving Google's general objections.

**REQUEST NO. 1:** State whether Google has intercepted or received communications from Wi- Fi networks in the United States while collecting data or communications for the Google Street View service, or at any other time during the specified time period. If the answer to this Inquiry is "Yes," respond to the Inquiries that follow herein.

**RESPONSE TO REQUEST NO. 1:**

Google passively received publicly broadcast Wi-Fi information in the United States using commercially-available Wi-Fi antennas and software from Wi-Fi networks within range of the Street View car, including data frames that may contain user communications in the payload portion of the data frame. Google refers to this information throughout these Responses as “payload.” The networks from which Google received such information were configured so that publicly broadcast Wi-Fi information (using the 802.11 standard) was readily accessible to the general public.

**REQUEST NO. 2:** State how many times Google intercepted or received Wi-Fi network communications, including the number of Wi-Fi devices from which communications were intercepted or received.

**RESPONSE TO REQUEST NO. 2:**

Google has not analyzed the payload data to determine how many communications were received.

Further, Google cannot reliably identify the number of Wi-Fi devices from which communications were collected. Google can identify the number of basic service set identifiers (also known as “BSSIDs”) which generally identify a single Wi-Fi access point that may be used by multiple stations, such as a laptop or other Wi-Fi-enabled device. The BSSID is the MAC address of the wireless access point, not the other devices, and does not indicate how many devices or networks connect through the access point itself. Google estimates that a total of

To be clear, this number indicates nothing about the number of users, networks, or devices from which communications may have been collected from any given access point. Nor does it indicate that payload data was collected from each access point. The BSSID is continuously broadcast whereas payload data would only have been captured if a user were sending or receiving information on an unencrypted network at the moment of collection. Finally, neither the BSSID nor any other Wi-Fi network information identified a specific person or address.

**REQUEST NO. 3:** State the period of time during which such communications were intercepted or received, including the beginning and ending dates, for each collection referenced in response to Inquiry number 2 above.

**RESPONSE TO REQUEST NO. 3:**

Google's collection activities described in response to Request No. 1 occurred between January 2008 and April 2010. Google has not analyzed the payload data to determine the date any individual communication was received.

**REQUEST NO. 4:** Separately for each instance in which communications were intercepted or received, provide a full explanation of the method and purpose of interception or reception, including but not limited to the following:

- a. full explanation of the purpose of the interception or reception and intended use of the communications;
- b. the range of radio frequencies over which communications were intercepted or received;
- c. the communications protocol utilized in intercepting or receiving the communications;
- d. the specific equipment and software tools utilized in intercepting or receiving the communications; if specialized software tools were developed to intercept or receive communications, describe the reason(s) for developing such tools;
- e. how the equipment functioned to intercept or receive the communications, including the frequency with which the equipment sampled the communications;
- f. how, if at all, Google correlated intercepted or received communications with the location, SSID, MAC address, or identity of the transmitter or user;
- g. the means by which the communications were stored once the interception or reception was accomplished; and
- h. the business unit and individuals responsible for authorizing the interception or reception of such communications.

**RESPONSE TO REQUEST NO. 4:**

- a. full explanation of the purpose of the interception or reception and intended use of the communications;

The Wi-Fi network data, as opposed to the payload data, that Google collected in the United States was used in the development of Google's geolocation server ("GLS"). The purpose of the GLS is to provide a user's approximate location based on a combination of GPS signals (where available) and signals received from cell towers and Wi-Fi networks visible to the relevant user's device. The GLS is, in turn, necessary to provide accurate location-based services, like Google Maps. The Wi-Fi network data is used to improve the coverage and accuracy of the longitude and latitude coordinates assigned to the MAC addresses contained in the GLS. Neither GLS nor Google's location-based services disclose the SSIDs or MAC addresses or other network data specific to a Wi-Fi access point (although a user's device is able to detect these data independently).

Location-based services, such as Google Maps navigation, use GLS. For example, users of Google Maps for mobile phones can turn on the "My Location" feature which will send a query



to GLS in order to identify the user's approximate location based on GPS signals (where available) and the signals from cell towers and Wi-Fi networks currently visible to their mobile phone. Such features generally work as follows:

- The user's device sends a request to Google with a list of MAC addresses or cell tower IDs currently visible to the device.
- GLS compares the MAC addresses or cell tower IDs from the device with a list of known MAC addresses or cell tower IDs associated with a geolocation.
- GLS then uses the geolocation to provide an approximate location (by latitude and longitude) of the user and sends it back to the user's device.

Again, the data on the server (the SSID, the MAC addresses and the other network data in relation to a Wi-Fi access point) is never disclosed by the GLS system or by the geolocation services operated by Google.

As to the collection of the payload data itself, no member of senior management and no product group asked for payload to be collected and it was not included in any product or service. The Wi-Fi project arose in mid-2007, when an engineer (the "Engineer") working on Wi-Fi-related issues in Google's Mountain View, California, offices heard about the plans for Street View. He believed he could provide a useful system to collect publicly broadcast Wi-Fi signals while the Street View cars drove the streets for use in location-based services. His manager, who was also the technical engineering lead for the Street View project, thought the idea was a good one and that Street View cars could serve as an ideal platform for this collection even though the collection of Wi-Fi signals had nothing to do with the Street View project itself.

The Engineer commenced the project by outlining in a design plan document the way he planned to go about building the capability, the equipment he needed, and the software he would write. He noted in the document that the software would collect Wi-Fi network data like MAC address and SSID that would be very useful in location-based services. He also wrote that "web traffic" – which we understand today means the payload -- would be collected and could be useful for search quality analysis, although he expected whatever the payload information collected to be highly fragmented due to the channel hopping technique he employed and the mobility and speed of the cars. Finally, he wrote that the collection would not have significant privacy impact because the Wi-Fi network data would not personally identify anyone or the precise physical location or address of the detected Wi-Fi access point. The design documents are identified as confidential and proprietary, and provided in response in Request No. 11 (marked as Documents 11-1 and 11-2).

The design document and the code the Engineer eventually wrote were made available to others to review if they so desired, but the significance of the Engineer's reference to "web traffic" was not appreciated. The Engineer thought it was appropriate to collect any publicly broadcast Wi-Fi information, including the payload from unencrypted networks, and that it might be useful in the future. Google disagrees with him on both points. It was not appropriate to include a function in the software to store payload from unencrypted networks and the information was not useful in any way. The payload served no purpose, was not used in any product or service, and despite the

*Unredacted Copy – Subject to Request for Confidential Treatment*

Engineer's initial and subsequently rejected idea about potential use, Google never had any intended use for it. No payload data collected in the United States has been disclosed to any person.

The code developed by the Engineer and incorporated into the onboard Street View car computer system is identified as confidential and proprietary, and provided in response to Request No. 11 (marked as Document 11-3).

- b. the range of radio frequencies over which communications were intercepted or received;
- c. the communications protocol utilized in intercepting or receiving the communications;
- d. the specific equipment and software tools utilized in intercepting or receiving the communications; if specialized software tools were developed to intercept or receive communications, describe the reason(s) for developing such tools;
- e. how the equipment functioned to intercept or receive the communications, including the frequency with which the equipment sampled the communications;
- f. how, if at all, Google correlated intercepted or received communications with the location, SSID, MAC address, or identity of the transmitter or user;

We enclose a copy of the report prepared by an independent technical services firm, Stroz Friedberg LLC, which describes in detail how the Wi-Fi equipment and software operate, the frequencies and protocols covered, and the type of information collected ("the Stroz Friedberg Report"). The Stroz Friedberg Report is provided in response to Request No. 11 (Document 11-4). Google provides the following information to supplement the Stroz Friedberg Report and to respond to the Bureau's specific questions.

The Google Street View cars were fitted with Wi-Fi antenna equipment attached to the roof. [REDACTED]

[REDACTED] This antenna equipment receives publicly broadcast Wi-Fi radio signals within range of the vehicle. For additional information, the manufacturer's product page and data sheet can be found here:

[REDACTED]

The Wi-Fi antenna passively received the publicly broadcast radio signals using open source Kismet software. Documentation for the Kismet software is available at <http://www.kismetwireless.net/documentation.shtml>. The data was then relayed to Google-developed software that processed the data for storage. The Google software was designed to recognize encrypted networks and never to store payloads from those networks.

As explained in the Stroz Friedberg Report, the software Google used captured, parsed and wrote to disk 802.11 wireless frame header data and associated it with GPS coordinates of the car and timestamp when the Wi-Fi signal was received for storage and use in mapping network



locations. The Wi-Fi network data and related information that Google collected includes:

- SSID, or “service set identifier”
  - MAC Address
  - Signal strength
  - Data rate
  - Type of encryption method
  - Radio channel and protocol (e.g., IEEE 802.11b/g/n)
- g. the means by which the communications were stored once the interception or reception was accomplished;**

Google addresses Request No. 4(g) in regard to how data was stored below in response to Request No. 5.

- h. the business unit and individuals responsible for authorizing the interception or reception of such communications.**

No member of senior management and no product group asked for payload to be collected and it was not included in any product or service.

**REQUEST NO. 5:** Provide a full explanation of the treatment of the communications following interception or reception, including but not limited to the following:

- a. the methods by which the communications were stored or secured, if any, including whether the intercepted communications were encrypted before being stored;
- b. whether the communications have been analyzed by any automated mechanism or reviewed by any employee, agent, officer, or director of Google and, if so, describe each mechanism and/or identify each individual who has done so by name and describe with particularity his or her responsibilities and/or participation in such analysis or review;
- c. whether, how, and to what extent any automated mechanism or employee, agent, officer, or director of Google examined the physical address information, IP information, protocol/port information, application information, or content of intercepted communications;
- d. whether the communications have been analyzed or reviewed by any individual other than an employee, agent, officer, or director of Google and, if so, identify each individual who has done so by name and describe with particularity his or her responsibilities and/or participation in such analysis or review;
- e. whether the existence, contents, substance, purport, effect or meaning of the communications, or any summary or analysis thereof, have been published or divulged to any person or entity (whether intentional or not), including employees and contractors of Google; and
- f. whether any of the communications have been used for the benefit of any person or entity, or used in any way; if so, describe with particularity the manner in which the data or communications have been used.

**RESPONSE TO REQUEST NO. 5:**

- a. the methods by which the communications were stored or secured, if any, including whether the intercepted communications were encrypted before being stored**

All Wi-Fi information was initially stored on a hard disk located in the Street View car. The data was held in machine-readable format only. The data requires Google proprietary software to view it. The disk was then shipped to a warehouse to be forwarded to a secure Google data center facility to be uploaded onto Google servers. The payload information was stored as raw, aggregate, and unprocessed data in machine-readable format only on Google servers until Google removed it to ensure its security upon learning about this collection activity.

At this point, the payload data resides on encrypted hard drives, with U.S. data segregated from the rest of the world. These hard drives are securely stored and only Google's independent consultants have the encryption key.

Because Google ceased processing disks received from Street View cars in May 2010 shortly after it learned of the collection activity, some Wi-Fi data (including payload data) remains on disks. These disks are currently stored securely in Google's data center.

- b. whether the communications have been analyzed by any automated mechanism or reviewed by any employee, agent, officer, or director of Google and, if so, describe each mechanism and/or identify each individual who has done so by name and describe with particularity his or her responsibilities and/or participation in such analysis or review**

On one occasion in early 2008 (we have not been able to determine the exact date other than it was early on in the project), the Engineer who developed the code examined the data collected and stored on the Google File Server ("GFS") to determine whether it had any use. He wrote a program to search for URL strings in the payload and identified the presence of such data. The Engineer purportedly informally asked a member of Google's search quality team whether the data would be useful and was told it had no value. Having determined that there was no useful purpose for it, he did not access it again. Nor did he take the time to rewrite the code to discontinue the collection. In fact, he had little further involvement in the project, having moved on to another assignment.

The second instance when payload data was accessed was when Google became aware that payload data may have been collected from unencrypted Wi-Fi networks and our engineering staff confirmed that this was the case. In no other instance has any employee, agent, officer, or director of Google analyzed the collected data, nor has the collected data ever been analyzed by Google by any automated mechanism.

- c. whether, how, and to what extent any automated mechanism or employee, agent, officer, or director of Google examined the physical address information, IP**

**information, protocol/port information, application information, or content of intercepted communications**

Other than as described above, Google has not conducted an analysis of the payload data collected.

- d. whether the communications have been analyzed or reviewed by any individual other than an employee, agent, officer, or director of Google and, if so, identify each individual who has done so by name and describe with particularity his or her responsibilities and/or participation in such analysis or review**

The collected U.S. data described above has not been analyzed or reviewed by any individual other than as described above.

- e. whether the existence, contents, substance, purport, effect or meaning of the communications, or any summary or analysis thereof, have been published or divulged to any person or entity (whether intentional or not), including employees and contractors of Google**

Google has not disclosed payload data from the United States to any person.

- f. whether any of the communications have been used for the benefit of any person or entity, or used in any way; if so, describe with particularity the manner in which the data or communications have been used**

Google has not used payload data in any product or service, nor has such data been used for the benefit of any person or entity in any way.

**REQUEST NO. 6:** To the extent Google has analyzed the communications in any way, provide a full description of the analysis, including but not limited to the following:

- a. whether the users transmitting communications scrambled or encrypted the communications prior to the time of interception or reception; if so, identify the quantity and nature of the communications that were scrambled or encrypted, and those that were not scrambled or encrypted;
- b. whether the communications included data packets carrying voice- or video-related data;
- c. whether any communications by wire were intercepted or received;
- d. whether any identifiable personal, financial or password-related information was intercepted or received;
- e. whether any other intelligible information was intercepted or received; and
- f. the quantity of communications intercepted or received from particular sources (i.e., single networks or Wi-Fi routers), and as a whole.

**RESPONSE TO REQUEST NO. 6:**

Google has not analyzed the payload data collected in the United States other than as described above and therefore cannot respond to Request Nos. 6(a), (b), (d), and (e).

Google's response to Request No. 6(c) is no.

In response to Request No. 6(f), in the United States, approximately 200 gigabytes of payload data was collected. Google has not analyzed the payload data collected in the United States other than as described above and therefore cannot respond with respect to collections from particular sources.

**REQUEST NO. 7:** Provide the current status of the communications intercepted or received, including but not limited to the following:

- a. whether Google currently possesses the communications;
- b. whether any of the communications have been destroyed, and, if so, identify each individual who has done so (or directed that someone else do so) by name, and describe with particularity his or her responsibilities and/or participation in such destruction, provide the date of the destruction, and describe with particularity the reason or justification for such destruction; and
- c. whether the communications were scrubbed of personally identifiable information at any point;
- d. if Google possesses the communications as of the date of this letter, Google is instructed to provide a copy of or access to those communications;

**RESPONSE TO REQUEST NO. 7:**

See Response to Request No. 5. Payload data for the United States has been preserved as noted above. Payload data collected outside the United States has been deleted at the direction of regulatory authorities in Ireland, Denmark, Austria, Hong Kong, and the United Kingdom, and is in the process of being deleted at the direction of regulatory authorities in Canada.

In regard to Request No. 7(d), which requests access to the payload data collected in the United States, Google has not disclosed the U.S. payload to anyone, nor has Google itself analyzed the payload other than as described in response to Request 5(b). The payload data is subject to Google's preservation obligations in various other proceedings. Google believes that it is not prudent or necessary for any governmental authority to examine the communications and personal information of U.S. citizens in order to resolve this matter. Doing so in our view would only compound the privacy concerns caused by Google's collection in the first place. Apart from these prudential considerations, we believe that the law simply doesn't permit it.

Section 605 of Title 47 prohibits the disclosure of wrongfully intercepted communications or use thereof for benefit or gain. While Google believes that the collection was lawful under federal and state laws, nonetheless, the States, civil plaintiffs, and other regulatory agencies continue to



analyze the facts and it has not definitively been decided by competent and binding authority that no violation of the law occurred.

Accordingly, disclosure of the U.S. payload data to a governmental authority or third party might give rise to claims that there were additional violations of the law. The prohibition in Section 605 on disclosure is unequivocal. There are no exceptions. As the first clause of Section 605 demonstrates, Congress made exceptions for legal process in a specific circumstance, but made no such exceptions in regard to the second and third clauses, which are the only provisions of Section 605 potentially applicable here. When Congress says the disclosure cannot be made "to any person," that phrase under Section 605 has been construed to include any governmental entity or law enforcement person for over 70 years -- in other words, it is settled. *See Nardone v. United States*, 302 U.S. 379, 381-84 (1937) (Section 605 prohibited wiretapping by federal agents).

Apart from Section 605 of Title 47, Title 18 contains unequivocal prohibitions on the disclosure of wrongfully intercepted communications. Again, we believe that there is no violation of federal law, but that is exactly the gravamen of the federal investigations -- to determine if there is such a violation -- and those are the claims made in the civil litigation. Specifically, Section 2511(1)(c) of Title 18 makes it unlawful when any person "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection." An administrative subpoena issued by a federal agency would be insufficient to compel disclosure in any event.

**REQUEST NO. 8:** State whether any of the individuals or entities whose communications were intercepted or collected gave authorization to Google to do so. If so, provide any and all Documents and Correspondence relating to such authorization(s).

**RESPONSE TO REQUEST NO. 8:**

Wireless networks using the 802.11 standard publicly broadcast information that is readily accessible to the general public unless the user configures his or her network to prevent such access. Network owners can choose to make the network open (not secured by encryption such that a user's activity is accessible to others) or closed (secured by encryption so that payload is not accessible by authorized devices). Wireless modems come with built-in encryption capability and easy instructions so that users may readily configure their networks to be secure if they so choose. Many network owners, such as in coffee shops or public places, choose to have open networks as a convenience to their customers.

Unless users encrypt their wireless network, they make the Wi-Fi information readily accessible to the general public. To the extent the Letter asks whether Google nonetheless obtained individualized consent from network owners to receive Wi-Fi information while driving the Street View cars, the answer is that Google did not obtain such consent.

**REQUEST NO. 9:** Describe any remedial measures that have been implemented by Google to address interception or reception of communications as described in response to the preceding inquiries. Specifically, describe in detail the changes Google has made -- or intends to make -- to improve its internal privacy and security practices, including those mentioned in the October 22, 2010, Google blog posting.

**RESPONSE TO REQUEST NO. 9:**

As soon as Google learned of the mistaken collection, it grounded its cars and as noted above, took steps to secure the payload data. Google physically removed Wi-Fi equipment from all of its cars globally and has had an independent forensic consultant audit the Street View vehicles, equipment and software to ensure that no further Wi-Fi collection will occur as part of the Street View project. We enclose a copy of the report prepared by an independent consultant documenting the results of its inspection. The report is confidential and proprietary, and provided in response to Request No. 11 (Document 11-5).

As to the changes discussed in its October 22, 2010, blog post, Google is in the process of preparing a report of its process changes and improvements. We expect to complete this report and to submit it as a supplement to this response early next week.

**REQUEST NO. 10:** Provide any additional information that you believe may be helpful in our consideration and resolution of this matter.

**RESPONSE TO REQUEST NO. 10:**

Some have suggested that Google intended to collect Wi-Fi communications. If Google's intent was to collect large volumes of payload data or to use it in any meaningful way, it is hard to imagine or design a less effective way to do it. Because of the way the data was collected -- driving as opposed to static collection; channel shifting 5 times per second, etc. -- whatever was collected would generally be in fragmented form and of little utility to Google. Instead, the primary value in this program was the collection of publicly available Wi-Fi network information and it was ill-thought out and of no use to Google for the Engineer to include code to collect payload from unencrypted networks.

As these responses show, Google's data collection in the United States involved the passive reception of publicly broadcast Wi-Fi information, and Google has not disclosed that data to any person and has not used that data in any product or service, nor has such data been used for the benefit of any person or entity in any way. Consequently, Google did not violate Section 605.

**REQUEST NO. 11:** Provide copies of all Documents that provide the basis for or otherwise support the responses to Inquiries 1-10, above.

**RESPONSE TO REQUEST NO. 11:**

Google has not undertaken a comprehensive review of email of potential record custodians. As stated above, no one in senior management or the product teams requested that payload be collected, and it was not used in any product or service. A comprehensive email review to prove the absence of documents related to the collection would be a time-consuming and burdensome task. Google is providing a comprehensive response that shows a lack of knowledge and accordingly requests that it not be required to conduct a further email search at this time to in essence prove a negative. Other agencies have agreed with this approach, reserving the right to renew the request if not otherwise satisfied with the information provided.

Google is providing redacted versions of design plans and code, removing the identity information of the engineers. Google requests that it not be required to disclose the identities of its employees at this time. The identity of these individuals has not been publicly disclosed, and Google has not provided the information to foreign regulators who seek to interview these employees, nor has it provided the information to the Federal Trade Commission or State Attorneys General. We believe the identity of the employees at this stage serves no useful purpose with respect to whether the facts and circumstances give rise to a violation of Section 605. Google requests the Bureau's forbearance at this time, recognizing it may renew its request if it deems it necessary in the future.

Google provides the following documents:

Redacted Design Plans (Documents 11-1 and 11-2)

Redacted gStumbler Code files (Document 11-3)

Stroz Friedberg Report – Source Code Analysis of gStumbler (Document 11-4)

Report of Inspection and Remediation of Google Street View Vehicles' 802.11 Wireless Network Traffic Capture Capabilities (Document 11-5)





**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

December 14, 2010

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W., Room TW-A325  
Washington, DC 20554

Attn: Mindy Littell  
Investigations and Hearings Division  
Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

Re: **Google Inc., File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google") hereby supplements its responses, submitted December 10, 2010, to the letter dated November 3, 2010 from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission, which requests information about Google's collection of data from Wi-Fi networks in the United States.

Kindly contact me should there be any questions regarding this submission.

Respectfully submitted,



E. Ashton Johnston  
*Counsel for Google Inc.*

Enclosures

cc: Hillary DeNigro, Investigations and Hearings Division, Enforcement Bureau  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau



DOCUMENT 11-6

**CONFIDENTIAL REPORT BY GOOGLE INC.  
REGARDING THE COLLECTION OF PAYLOAD DATA USING STREET VIEW CARS  
AND PRIVACY ASSURANCE IMPROVEMENTS**

December 2010

## **I. BACKGROUND**

In 2006, Google Inc. ("Google") launched its Street View project to enhance users' experience in Google Maps and Google Earth with 360-degree street-level imagery of public spaces and privately-owned properties that have granted appropriate access to Google. These panoramic images promote greater understanding of a particular location and, among other things, provide useful geographic context. Today, users around the world enjoy the benefits of Street View to help them locate and find more information about local businesses; enrich driving directions; assist in both the sale and purchase of real estate; and promote tourism. At the same time, Google's success -- with Street View and all of its products -- depends on the continued trust of its users. In order to earn and maintain such trust, Google takes privacy concerns seriously and the Street View project is no exception.

Beginning in 2007, Google's Street View cars were fitted with commercially-available WiFi antennas and software to passively collect the publicly broadcast SSIDs, MAC addresses and other network information, which when combined with the GPS location of the cars collecting the data, help improve our location-based services. Such information is widely used by companies offering similar services. This WiFi network information does not and was not used by Google to identify any specific individual or household.

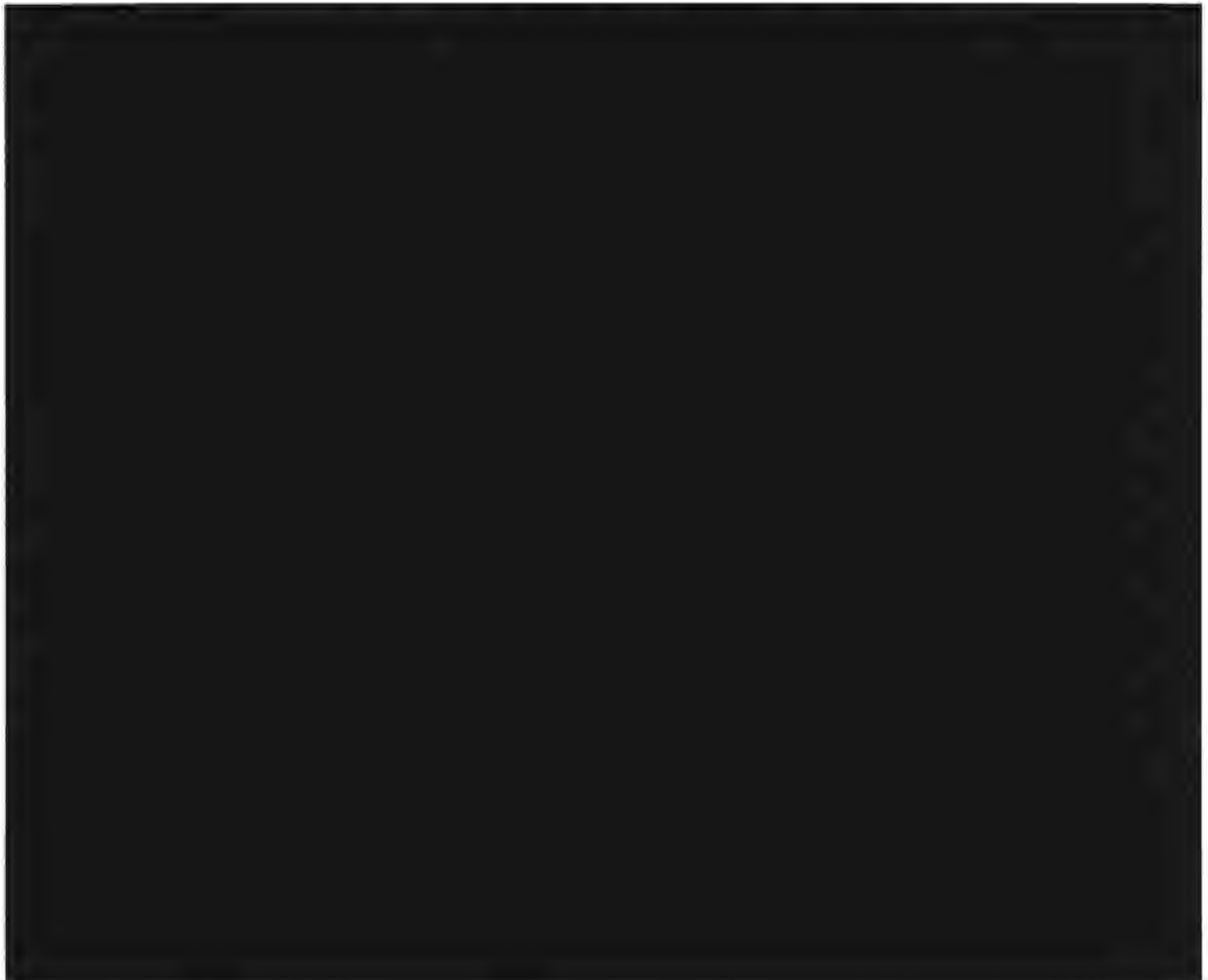
In addition, Google mistakenly included code in our software that collected payload data (information sent over the network) from unencrypted WiFi networks. The engineer who designed the code did so as part of a program that permits Google engineers to work on engineering projects of interest to them. The code worked with commercially-available WiFi antennas and open source code known as Kismet. The code was reviewed for bugs and validated by another engineer before being adopted and installed on Street View vehicles in late 2007. While this ensured that the code did not interfere with regular Street View operations, the review did not otherwise analyze the code for its functionality. As we now know, however, that code also stored data frames, including payload, from unencrypted networks. Once the payload data was discovered, Google requested an independent security firm to analyze the code and confirm its operation and the types of data collected. A copy of the report by Stroz Friedberg LLP is attached as Appendix A.

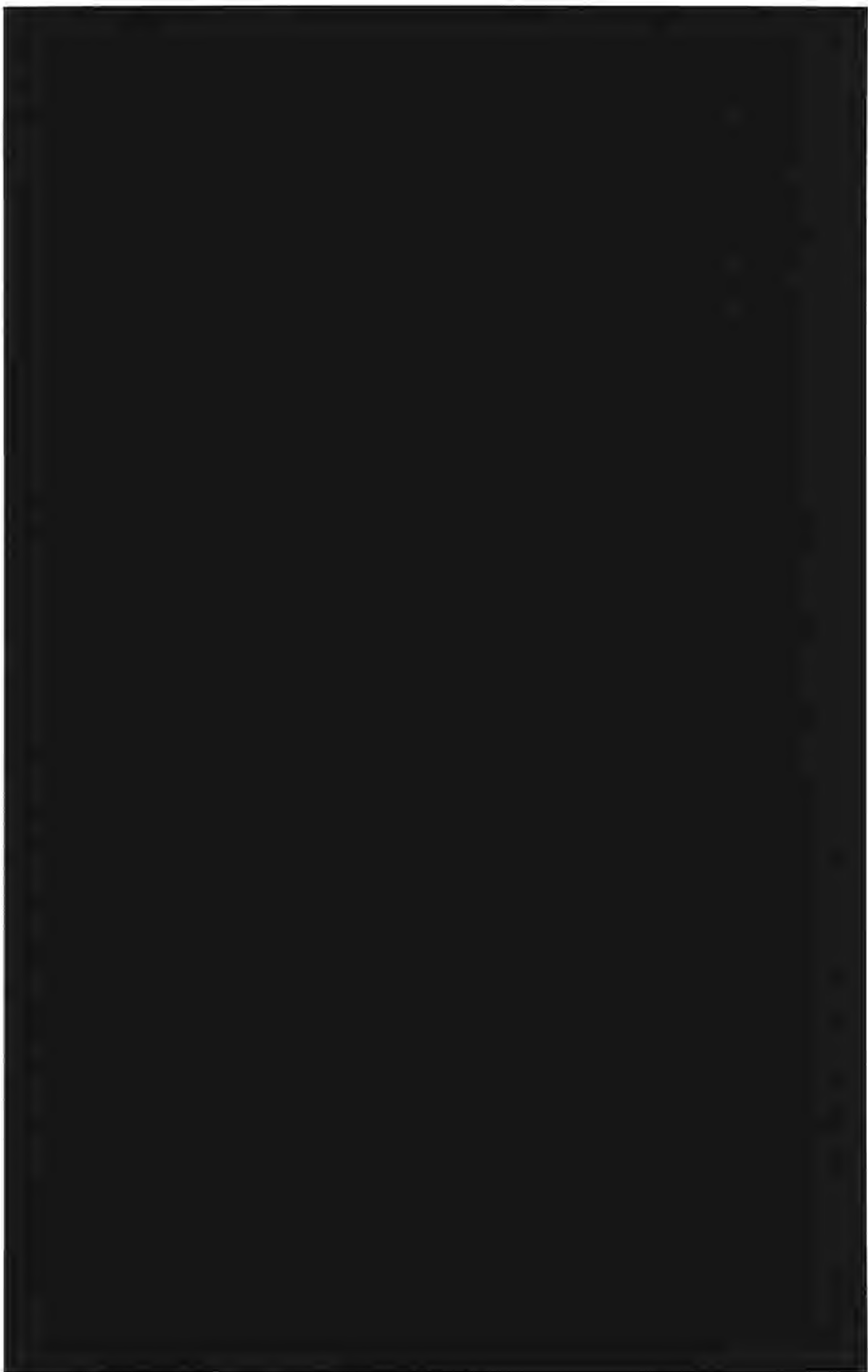
The WiFi network data was collected for use in Google's location-based services and was not

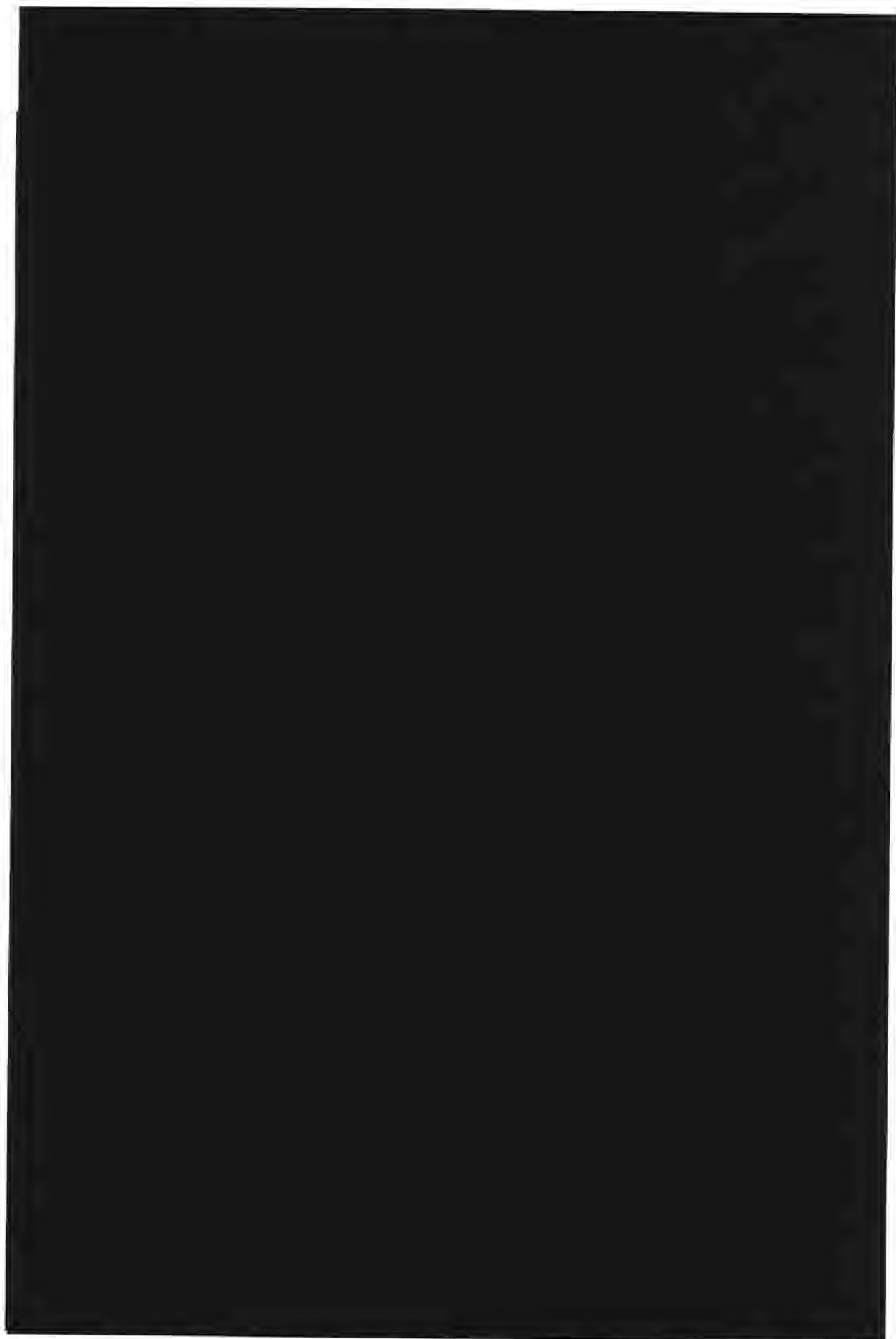
used in connection with the Street View project. To this day, while Google has acknowledged that the unencrypted payload data might contain communications, including URLs, emails or other personal information, Google has not performed a detailed analysis of the payload data itself.

Immediately upon learning that payload data had been collected, Google stopped driving the Street View cars, segregated the payload data on Google's network, and made it inaccessible to anyone other than the engineers responsible for securing it. We have determined that payload data was never used in any Google product or service or shared with any third party and no member of senior management or members of any product team asked for or wanted the payload information. Google is also ensuring the removal of all WiFi hardware and software from its Street Vehicles before starting to drive in the future. A copy of the report by Stroz Friedberg LLP confirming the protocol for removing the WiFi equipment and software is attached as Appendix B.

The failure of communication between the engineer, the product teams and the legal team is unfortunate and a mistake that Google is revamping its systems to avoid in the future. The following report describes our plan for improving Google's Privacy Assurance Program.























the 1990s, the number of people in the world who are obese has increased by 100% (World Health Organization 2000). The prevalence of obesity in the United States has increased from 15% in 1980 to 30% in 1998 (Flegal et al. 2000). In the United Kingdom, the prevalence of obesity has increased from 10% in 1980 to 16% in 1998 (Health Survey for England 2000). The prevalence of obesity in children has also increased in the United States (Flegal et al. 2000) and in the United Kingdom (Health Survey for England 2000).

Obesity is a major risk factor for a number of chronic diseases, including type 2 diabetes, coronary heart disease, stroke, and certain types of cancer (World Health Organization 2000). Obesity is also a risk factor for a number of mental health problems, including depression and anxiety (Flegal et al. 2000). Obesity is a complex condition, and its development is influenced by a number of factors, including genetics, environment, and lifestyle.

One of the most important factors influencing the development of obesity is diet. A diet that is high in calories and fat, and low in fiber and other nutrients, can lead to weight gain. A diet that is high in fiber and other nutrients, and low in calories and fat, can help to prevent weight gain. Exercise is also an important factor in the development of obesity. Regular exercise can help to burn calories and build muscle, which can help to prevent weight gain.

Obesity is a complex condition, and its development is influenced by a number of factors. However, diet and exercise are two of the most important factors. A diet that is high in calories and fat, and low in fiber and other nutrients, can lead to weight gain. A diet that is high in fiber and other nutrients, and low in calories and fat, can help to prevent weight gain. Regular exercise can help to burn calories and build muscle, which can help to prevent weight gain.

Obesity is a complex condition, and its development is influenced by a number of factors. However, diet and exercise are two of the most important factors. A diet that is high in calories and fat, and low in fiber and other nutrients, can lead to weight gain. A diet that is high in fiber and other nutrients, and low in calories and fat, can help to prevent weight gain. Regular exercise can help to burn calories and build muscle, which can help to prevent weight gain.

Obesity is a complex condition, and its development is influenced by a number of factors. However, diet and exercise are two of the most important factors. A diet that is high in calories and fat, and low in fiber and other nutrients, can lead to weight gain. A diet that is high in fiber and other nutrients, and low in calories and fat, can help to prevent weight gain. Regular exercise can help to burn calories and build muscle, which can help to prevent weight gain.

Obesity is a complex condition, and its development is influenced by a number of factors. However, diet and exercise are two of the most important factors. A diet that is high in calories and fat, and low in fiber and other nutrients, can lead to weight gain. A diet that is high in fiber and other nutrients, and low in calories and fat, can help to prevent weight gain. Regular exercise can help to burn calories and build muscle, which can help to prevent weight gain.

Obesity is a complex condition, and its development is influenced by a number of factors. However, diet and exercise are two of the most important factors. A diet that is high in calories and fat, and low in fiber and other nutrients, can lead to weight gain. A diet that is high in fiber and other nutrients, and low in calories and fat, can help to prevent weight gain. Regular exercise can help to burn calories and build muscle, which can help to prevent weight gain.

## Appendix A





## **Source Code Analysis of gstumbler**

Prepared for Google and Perkins Cole  
Prepared by STROZ FRIEDBERG  
June 3, 2010



## **Table of Contents**

I.	Introduction	1
a.	Executive Summary	2
b.	Basic Technical Descriptions and Definitions	2
c.	Overview of Findings	4
II.	Overview and History of gstumbler, gslite, and Kismet	5
III.	Scope of Review and Methodology	7
IV.	Detailed Analysis and Findings	8
a.	Source Code Flow and Functionality	8
b.	Frame Parsing	10
c.	Default Settings Governing Discard of Data and Writing to Disk	11
d.	GPS Interpolation	12
e.	Command Line Arguments in Configuration Files	13
V.	Conclusion	13
APPENDIX A – Source Code Inventory		14
APPENDIX B – 802.11 Frame Elements		16
APPENDIX C – Protocol Buffer Messages		19

## **I. Introduction**

1. Stroz Friedberg, LLC ("Stroz Friedberg") is a consulting and technical services firm that specializes in digital forensics, data breach and cyber-crime response, on-line and traditional investigations, and electronic discovery. The firm was founded in February 2000 by Edward M. Stroz. For ten years, Mr. Stroz has been a leader in the computer security and digital forensics field, and has pioneered the use of a blend of behavioral science and digital forensics in addressing the insider threat. Before founding what was then Stroz Associates, Mr. Stroz founded and then ran the Computer Crimes Unit of the F.B.I.'s New York office during his sixteen year career with the Bureau. Eric Friedberg, Mr. Stroz's Co-President at Stroz Friedberg, hails from the U.S. Attorney's Office in the Eastern District of New York, where he was the lead cyber-crime prosecutor and the Chief of the Narcotics Unit during his eleven year tenure as an Assistant United States Attorney there. Mr. Friedberg is an expert in cybercrime response, computer forensic investigations, and electronic discovery. Messrs. Stroz and Friedberg, together with the firm's Executive Management, manage the firm's operations. Stroz Friedberg's principal offices are in New York (HQ), Los Angeles, Washington, D.C., London, Dallas, Minneapolis, San Francisco, and Boston. The firm has handled many significant, high-profile digital forensics matters, including a number of source code analyses in the civil, regulatory, and criminal arenas. Mr. Friedberg led the team that conducted the source code analysis in this case.

2. Stroz Friedberg was retained by Perkins Cole, on behalf of Google, to evaluate the source code of an executable deployed on the vehicles otherwise collecting data for Google's Street View service offerings. Specifically, we were asked to provide a third-party assessment of the functionality of the source code for a Google project named "gstumbler" and its main binary executable, "gslite," with particular focus on the elements of wireless network traffic that the code captured, analyzed, parsed, and/or wrote to disk. Stroz Friedberg has no stake in the outcome of this matter and has been asked by Google and Perkins Cole to render a neutral, technical opinion regarding the functionality of gstumbler. Stroz Friedberg is being compensated on a time and materials basis. The project team consisted of three primary examiners/code reviewers and two engagement managers, and our report was internally peer-reviewed by others in the firm.

3. Between May 20 and May 26, 2010, Stroz Friedberg received the gslite source code from Google. The gslite source code is comprised of approximately thirty-two source code files, along with twelve additional files including configuration files, shell scripts, source code repository changelog information, binary executables, and kernel modules. A full inventory of the reviewed source code files and shell scripts is provided in Appendix A. It is our understanding that the provided source code and accompanying shell scripts represent the most current version of the gstumbler application deployed as of May 8, 2010, on vehicles otherwise capturing data for Google Street View. Our findings regarding the application's functionality, based upon our review of the source code, are set forth below: first, in the Executive Summary, and then more specifically in the Overview of Findings and the body of this report.

#### **A. Executive Summary**

4. The executable program, gslite, works in conjunction with an open source network and packet sniffing program called Kismet, which detects and captures wireless network traffic. The program facilitates the mapping of wireless networks. It does so by parsing and storing to a hard drive identifying information about these wireless networks – including but not limited to their component devices' numeric addresses, known as MAC addresses, and the wireless network routers' manufacturer-given or user-given names, known as "service set identifiers," or "SSIDs." The "parsing" involves separating these identifiers into discrete fields. Gslite then associates these identifiers with GPS information that the program obtains from a GPS unit operating in the Google Street View vehicle. Gslite captures and stores to a hard drive the header information for both encrypted and unencrypted wireless networks.

5. While gslite parses the header information from all wireless networks, it does not attempt to parse the body of any wireless data packets. The body of wireless data packets is where user-created content, such as e-mails or file transfers, or evidence of user activity, such as Internet browsing, may be found. While running in memory, gslite permanently drops the bodies of all data traffic transmitted over encrypted wireless networks. The gslite program does write to a hard drive the bodies of wireless data packets from unencrypted networks. However, it does not attempt to analyze or parse that data.<sup>1</sup>

#### **B. Basic Technical Descriptions and Definitions**

6. To understand the functionality of the gslite source code, and to understand the Overview of Findings set forth below in Section 1(C), it is important to understand the basic technical concepts critical to the architecture of wireless 802.11 networks and the transmission of data over such wireless networks.

7. Data is transmitted over the Internet via packet switching technology. Briefly, a communication transmitted via the Internet is broken up into "packets" at the point of origination, and the packets of data are routed from the originating device to various other computer devices on the Internet until they reach their final destination. Each packet is comprised of a packet header which contains network administrative information and the addressing information (or "envelope" information) necessary to transmit the data packet from one device to another along the path to its final destination. Each packet also contains a "payload" which is a fragment of the "content" of the communication or data transmission sent and received over the Internet; payload information can include, for example, fragments of requests for URLs, files transferred across the Internet, email bodies, and instant messages, among other things. The packets associated with a particular data transmission may travel over different routes across the Internet to reach their final destination; once they reach the destination device, the packets are reassembled to create the entire transmission.

8. A router is a device on a network that receives a data packet and transmits it to the next router or device on the network. A MAC address is a unique number assigned to a piece of networking hardware, such as a router, by that hardware's manufacturer. Each device and router on a wireless network has a MAC address uniquely identifying that machine.

9. Packets are encapsulated into larger data packages called frames for routing over various network types. Multiple specifications for the transmission of packets using frames have been promulgated by the Institute of Electrical and Electronics Engineers. This report focuses on

---

<sup>1</sup> From an analysis of the source code alone, we cannot ascertain the extent to which gslite captures of unencrypted wireless data would be fragmented or complete. Given the factors that the Google Street View Vehicles can be moving or stationary and, as discussed below, the Kismet device is set to hop rapidly between wireless channels, the numerous wireless data packets that constitute any single user communication may or may not be captured by Kismet.

data transmitted over wireless networks pursuant to the 802.11 protocols, the specifications for which provide the international standard for the transmission of data over wireless networks operating in the 2.4, 3.6, and 5 GHz frequency radio bands.

10. There are three primary types of 802.11 frames, which contain information necessary to transmit data packets from one device to another over wireless networks. The three types of 802.11 frames are Control frames, Management frames, and Data frames, each of which is described below:

a. *Control Frames* control access to particular types of networks and facilitate exchanges of Data frames between wireless links. Control frames send the Request to Send (RTS) and Clear to Send (CTS) messages necessary to establish a connection between two links on a network prior to transmitting a data packet (sometimes referred to as a "two-way handshake"). Control frames also transmit the Acknowledgement (ACK) information once a Data frame is received by a link. A diagram of a generic Control frame is provided in Appendix B.1.

b. *Management Frames* contain information necessary to manage a data transmission over the network. Management frames contain, for example, authentication information, information necessary to allocate resources to a transmission, data transmission rates, SSIDs (i.e., network names), information necessary to terminate a connection, and periodic beacon signals. These properties are stored, in part, as Information Elements, that is, id-value pairs in the payload of Management frames. A diagram of a generic Management frame is provided in Appendix B.2.

c. *Data Frames* serve the function of encapsulating and transmitting packets of data over wireless networks. Generally, the body of each Data frame contains the "content" data of the encapsulated packet transmitted over the Internet, including such user-created data as email header information and bodies, URL requests, file transfers, instant messages, or any other communication over the Internet, as well as the addressing information for such transmissions. A diagram of a generic Data frame is provided in Appendix B.3.

d. Each of these frame types have numerous subtypes, which determine, among other things, the fields present in the 802.11 frame. A frame's type and subtype information is stored in the *Frame Control* header field of the 802.11 frame, which is discussed in more detail below.

11. At a high level, an 802.11 frame can be considered to have two distinct sections: the header data and the body data. The header data is comprised of the Frame Control, duration or id, MAC addresses, sequence control number, and quality of service, or QoS, control information. The body data is comprised of the frame body component of an 802.11 frame, to the extent the frame's type and subtype calls for this field. As noted, the body of a Data frame may contain packet content data.

12. A diagram of a generic 802.11 frame showing its various components is below:

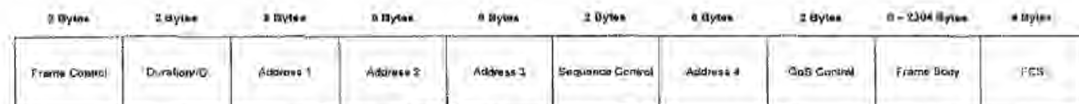


Figure 1. Generic 802.11 Frame Format.

The Frame Control, Duration/ID, Address, Sequence Control, and QoS control fields are considered the 802.11 *frame header*, while the frame body contains the payload data previously discussed. The FCS field contains checksum information used to confirm that the wireless frame was accurately received.

13. Every 802.11 frame contains a 16 bit Frame Control field that contains information regarding the status of the frame and the wireless transmitter of the frame. Specifically, the Frame Control field contains the following properties: Protocol Version; Type; Subtype; To DS; From DS; More Fragments; Retry; Power Management; More Data; Protected Frame; and Order. The Type field is a two bit field that will be 00, 01, or 10 to indicate if a frame is a Management, Control, or Data frame respectively, and the Subtype is a four bit field used to specify the frame's subtype. The To DS and From DS fields are single bit values that specify the routing of the 802.11 frame across the wireless network.

14. The Protected Frame bit in the Frame Control field is also known as the frame's "encryption flag." The Protected Frame field is a single bit which identifies whether the wireless network's transmissions are encrypted; it has no relation to the payload within any Data frame or whether that encapsulated packet transmission is itself independently encrypted. For example, if a fragment of a secure, encrypted HTTP session (HTTPS) were encapsulated in the payload of a Data frame on an unencrypted wireless network, the Data frame's encryption flag would still be set to "0", i.e. "false", indicating that the frame is unencrypted. The 802.11w-2009 amendment to the 802.11 specification, which was approved on September 11, 2009, provides a mechanism to also encrypt unicast Robust Management frames, which will result in the Protected Frame field being set to "1", i.e. "true."

15. Each 802.11 frame type contains at least one MAC address associated with the wireless local area network (LAN). 802.11 frames can contain up to four such MAC addresses associated with a particular wireless LAN.

16. Each wireless network has a public name, known as the SSID. The SSID name may be set by the owner of the wireless network. The SSID can be publicly broadcast to all wireless devices within its range. The broadcast feature also can be disabled so that the SSID for a particular wireless network is not readily visible to devices seeking wireless networks even though the SSID is still ascertainable from the transmitted packets.

17. The 802.11 wireless specifications divide each of the frequency bands into *channels*, analogous to TV channels. The division is regulated by individual countries, resulting in different locales having different numbers of permitted channels in each band. For example, in European countries, the frequency bands are regulated such that transmission is permitted across thirteen overlapping channels between 2.4 and 2.4835 GHz, each of which is 5 MHz apart and 22 MHz in width. A particular communication is transmitted over only one channel; thus, to the extent a packet sniffer is set to "hop" through channels—similar to changing a radio or TV channel—it may only collect fragments of a particular communication.

### **C. Overview of Findings**

18. Using the more technical terminology in the above section, we expand on our high-level findings.

19. As set forth above, the executable program, gslite, is an 802.11 wireless frame parsing and collection tool that associates GPS coordinates with wireless network frames. While running in memory, the program parses frame header information, such as frame type, MAC addresses, and other network administrative data from each of the captured frames. The parsing separates the information into discrete fields for easier analysis. In addition, per-packet information regarding the wireless transmission's strength and quality is captured and associated with each frame. All available MAC addresses contained in a frame are also parsed. All of this parsed header information is written to disk for frames transmitted over both encrypted and unencrypted wireless networks.



20. The gslite program discards the frame bodies of 802.11 Data frames sent over encrypted wireless networks. The program inspects the encryption flag contained in each frame header to determine whether the frame is encrypted, i.e., whether it is being transmitted over an encrypted wireless network. If the encryption flag identifies the wireless frame as encrypted, the payload of the frame is cleared from memory and permanently discarded. If the frame's encryption flag identifies the frame as not encrypted, the payload—which exists in memory in a non-structured bit stream of ones and zeros—is written to disk in a serialized format, as further described below.

21. The gslite program parses Management frame bodies and stores the parsed data as "Information Elements." The gslite program also parses Control frames' subtype information before writing it to disk. By contrast, gslite does not parse Data frames' bodies, which may contain user-created content. Rather, unencrypted Data frames' bodies pass through memory unparsed and are written to disk in their unparsed format. (Again, encrypted frame bodies are dropped entirely.)

22. As set forth above, the gslite source code includes logic that examines wireless frames' type and encryption status, and determines whether to discard them in whole or in part. The default behavior of gslite is to record all wireless frame data, with the exception of the bodies of encrypted 802.11 Data frames. The gstumbler application is configurable through the use of command line arguments that make it possible to specify, at the time the program is run, what types of wireless frames to record. Based on our review of the provided configuration files and shell scripts used to launch gslite, prior to May 6, 2010, the gstumbler application used the default configurations described above, which is to say that all wireless frame data was recorded except for the bodies of 802.11 Data frames from encrypted networks.<sup>2</sup>

## **II. Overview and History of gstumbler, gslite, and Kismet**

23. The source code reviewed is from a project referred to at Google as "gstumbler." According to internal Google documentation, gstumbler was first created and used in 2006. At that time, the program executable was itself also named "gstumbler," but at some point in or after late 2006, the executable deployed to vehicles otherwise capturing data for Google's Street View services was revised and renamed "gslite." The gslite program is the focus of this source code review. In this report, "gslite" refers to the specific executable program for which Stroz Friedberg reviewed the source code; and "gstumbler" refers to the overall application, including the configuration files and shell scripts that the Google Wifi project has used to detect and collect wireless network data.

24. The gslite source code is written in C++. C++ is an object oriented programming language, where objects are defined as data structures comprised of properties and methods, i.e. values and functions. An "object" refers to an instance of a data structure in memory. The gslite program makes use of object oriented programming to represent 802.11 frames in memory, parsing the raw frame data and storing its structural elements in a Dot11Frame object as defined in the source code file packet.proto. The Dot11Frame object is defined using a framework called Protocol Buffers, which was developed at Google to provide a means for writing complex data structures to disk. Protocol Buffers are discussed more fully in Appendix C.

25. The gslite program parses some, though not all, information from 802.11 wireless frames read in from a source of wireless frames. It simultaneously receives geolocation coordinates from a GPS system and then associates each wireless frame with the time and approximate location in which it was received. The gslite program works in concert with a second program, Kismet, which must run simultaneously. Kismet controls one or more wireless cards on a Google vehicle

---

<sup>2</sup> It is our understanding that on May 6, 2010, in response to regulatory attention, the gstumbler shell script was revised to disable all Data frame capture. We have inspected that revised shell script and have confirmed that revision.

and provides gslite with the stream of detected wireless frames. The relationship between gslite and Kismet is depicted in Figure 2.

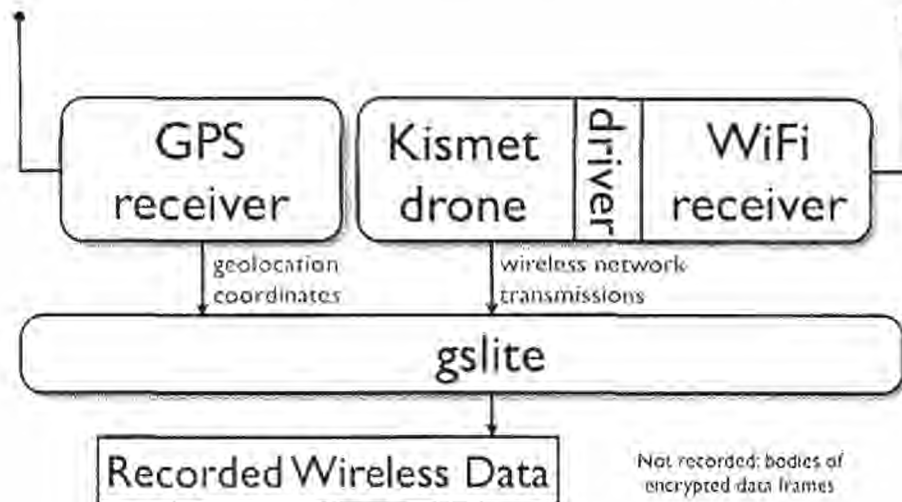


Figure 2. Inputs to gslite.

26. Kismet is a freely available, open-source application for wireless network detection and packet sniffing. Kismet captures wireless frames using wireless network interface cards set to monitoring mode. The use of monitoring mode means that Kismet directs the wireless hardware to listen for and process all wireless traffic regardless of its intended destination. Kismet captures wireless frames passively, meaning that that Kismet receives such transmissions without actively transmitting to nearby wireless networks. Kismet only detects packets passively. Through the use of passive packet sniffing, Kismet can also detect the existence of networks with non-broadcast SSIDs, and will capture, parse, and record data from such networks.

27. Kismet is a standalone application capable of capturing and filtering wireless frames. However, it can also be deployed in a configuration called a "drone," which does not record or analyze network traffic but instead forwards captured traffic to a server listening for such traffic. The Kismet drone program places a Kismet header describing the properties of the wireless transmission in front of the raw 802.11 frame and passes it to gslite for further processing. The gslite application listens for data from a Kismet drone running simultaneously within the Street View vehicle.

28. A Kismet drone is configured through the use of a file named `kismet_drone.conf`, which provides, among other things, instructions for Kismet to "channel hop." Channel hopping is the act of cycling through numerous 802.11 channels per second in order to capture frames from as many nearby networks as possible. In the `gstumbler` project, Kismet's configuration file is created using a predefined template file, and entries in Google's template instruct the drone to change wireless channels five times per second, as shown below (`kismet_drone.conf.template` lines 37-41):

```

# Do we channelhop?
channelhop=true

# How many channels per second to we hop? (1-10)
channelvelocity=5

```



As discussed above, the number of permitted channels for broadcast in a given frequency is regulated by a country's local authorities, and the number of permitted channels for broadcast in a frequency ranges between 11 and 14. The `kismet_drone.conf.template` file directs which channels should be monitored and the order through which they are hopped. In the United States, for example, there are 11 channels that may be used to wirelessly transmit data within the 2.4 Ghz band. Accordingly, when configured for the United States, Kismet listens to each of the 11 channels for one fifth of a second, thus listening to every channel for one 0.2 second interval during each 2.2 second channel hopping cycle.

### **iii. Scope of Review and Methodology**

29. Upon receipt of the `gslite` source code, Stroz Friedberg conducted a high-level review of the `gslite` framework code and associated modules. The purpose was to understand the basic logic flow and functionality of the program, and the significance and dependencies of the various components.

30. Based on our high level review, Stroz Friedberg identified key modules and dependencies for closer scrutiny, and assessed the significance of Google commands and code modules called from libraries external to the `gslite` code for use within the program. We received confirmation that particular functions and modules were borrowed from standard, shared libraries within Google. Because we also confirmed that such functions and codes were not customized for use in `gslite`, but were merely imported to perform standard functions, we focused on the core functionality and key programming modules unique to `gslite`.

31. We also did not independently review the Kismet program. As noted above, 802.11 frames initially are captured by the Kismet program, an open source packet sniffing program. It is our understanding based upon representations from Google that Kismet source code was not modified or adapted in any way as part of the `gstumbler` project.

32. We compared 802.11 frame specifications to the `gslite` frame parsing parameters encoded into the program to verify that the code's parameters are consistent with the specifications. That is, if the code parses particular bits of frame header information to determine, for example, the type of frame or whether the wireless network is encrypted, we confirmed that the program looks at the correct frame bits to parse the expected field from the raw data.

33. We closely scrutinized the parsing functionality of the `gslite` program as it pertains to each type of 802.11 frame. We determined how different types of frames are parsed, the different fields parsed for each frame type, what 802.11 frame fields are written to disk in parsed formats versus raw formats, and what 802.11 fields are discarded and not written to disk.

34. We analyzed the overall structure of code to determine the program's default behavior and the ways in which default behavior may be changed by command line arguments. We also examined the command line configuration settings over the course of `gslite`'s deployment.

35. We confirmed our understanding as to other secondary functions of the program, including its logic to detect bad frames and not process them, its diagnostic capabilities for assessing proper functioning of the program, its calculation and correlation of GPS geolocation information with detected wireless networks, and its decision as to how and when to write data to disk.

36. Stroz Friedberg did not receive or analyze earlier versions of the `gslite` source code or its predecessors. We did, however, review the modification history and did not observe significant changes to the program regarding how frames are parsed and recorded. We also reviewed all available versions of the shell scripts used to launch Kismet and `gslite` to verify what command line arguments were used.

#### IV. Detailed Analysis and Findings

##### A. Source Code Flow and Functionality

37. At the highest level of description, Google's gstumbler program creates a series of servers and objects that interface with the Google Street View vehicle's GPS system and the Kismet drone, pulls wireless frames from a stream provided by the Kismet drone, and then assigns timestamp and geolocation information to each wireless frame it encounters, saving the results to disk. The general description of how gstumbler operates is illustrated in Figure 3, below, and in the following paragraphs.

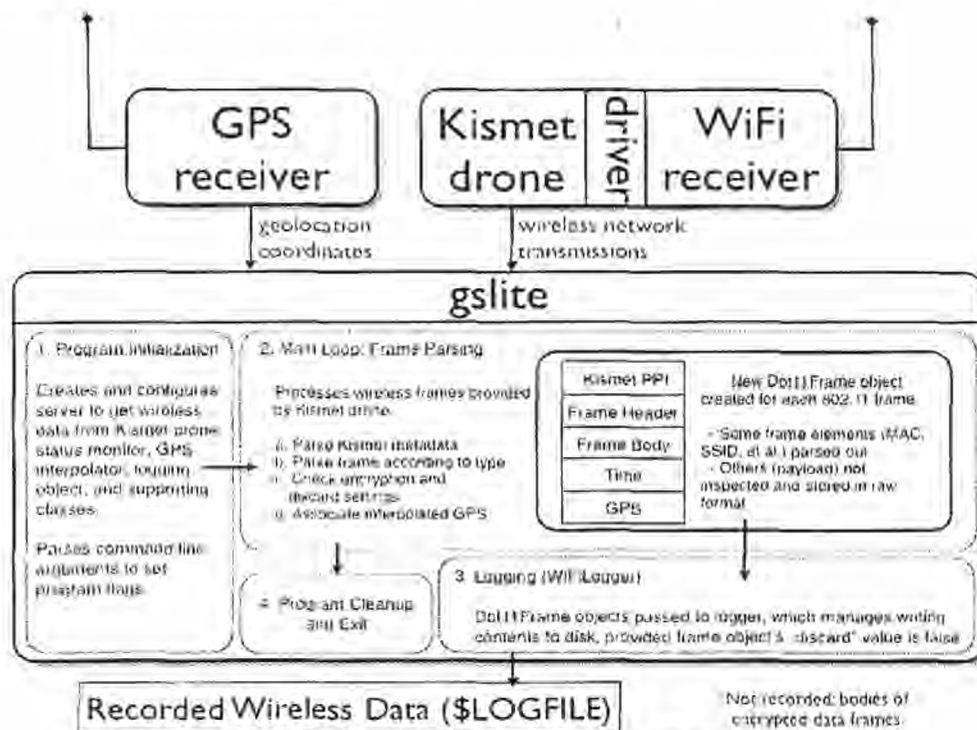


Figure 3: High-level representation of gslite program execution

38. The program first parses any command line arguments passed to it from the shell script, `run_gstumbler`, used to launch `gslite`. The program starts and configures a series of services, including, but not limited to: a `WifiRecordLogger`, which manages the storing of 802.11 frame data to disk; and a `WifiLiteServer` object, which listens for Kismet data on a predefined port.

39. For each frame being processed, the program creates a new `Dot11Frame` object in which to store the parsed 802.11 frame fields, along with a pointer to it. The `Dot11Frame` is a data structure that is built using Google's Protocol Buffers libraries. As noted previously, information about `Dot11Frame` objects and Protocol Buffers in general is provided in Appendix C.

40. The program parses the per-packet information (PPI) header information Kismet affixes to a captured 802.11 frame. PPI includes the quality of the signal, the signal strength, the signal noise, if the capture source indicated there was an error in the capture to Kismet, transmission channel, the signal carrier, the signal encoding, and the data transmission rate. The program

also sets the Dot11Frame's time received, time sent, and raw data properties to match those of the corresponding incoming frame.

41. The program proceeds to parse the 802.11 frame as described more fully in section B, below. The gslite program runs the Parse() method of a number of PacketParser objects against the incoming 802.11 frames: Dot11ParserImpl::Parse(); CtrlParserImpl::Parse(); MgmtParserImpl::Parse(); and TruncateParserImpl::Parse(). Although the forms of information available in a given frame vary according to its type and subtype, the packet parsers are applied to all frames regardless of type. The parsing process populates numerous properties of the Dot11Frame object with information extracted from the 802.11 frame. Parsing does not include inspection of the bodies of Data frames.

42. During the TruncateParserImpl::Parse() parsing function, gslite reads the encryption flag on each frame. That bit is located within the second byte of the Frame Control on an 802.11 frame. If the encryption flag is set to "true," then the frame's body, or payload, is cleared from memory and permanently discarded. If it is "false" the frame's body is retained for writing to disk.

43. The GPS Interpolator associates geolocation coordinates with the frame and writes the coordinates into the Position property of the Dot11Frame.

44. The parsed 802.11 frame object is written to disk using WriteProtocolMessage() method of the RecordWriter object. In the case of Management frames, the body is written to disk as parsed Information Elements, while in the case of unencrypted Data frames, the body is written to disk in unparsed format. It is our understanding based upon representations from Google that the RecordIO module, used to write the Dot11Frame objects to disk, is a common shared library within Google, and it is utilized unchanged in gslite.

45. The main loop of the program continues parsing, collecting, and geolocating each 802.11 frame as it is detected and forwarded by the Kismet drone. An interrupt signal sent from a user or from the operating system will cause the program to exit the main loop, clean up objects in memory, and exit.

46. The gslite program also writes logging information, largely regarding program status and error conditions, to a default system location. Our review found one line of code that, when executed, writes the content of a wireless frame to disk, through the use of a protocol buffer method for formatting a data structure as a string (scanner.cc lines 114-115):

```
if (!parser->Parse(frm)) {  
    LOG(ERROR) << "Error parsing frame: " << frm->ShortDebugString();
```

The second line of code above writes the wireless frame to disk, including its body, regardless of frame type or encryption flag. However, the program only performs this logging when a wireless frame cannot be successfully parsed and the Parse() method returns false. Our review of the Parse() method determined that this condition is met only when a frame's length is too short to constitute a valid frame header. In such an event, the frame also would be too short to contain a frame body. Furthermore, any such invalid frame would be discarded by Kismet or the wireless card prior to being forwarded to gslite. Accordingly, the circumstances necessary to invoke this logging action preclude the possibility that frame payload content would be written to the error log.

47. During execution, gslite also reports certain diagnostic information in HTML format to the HTTP server to provide in-vehicle feedback regarding the status and operating state of gslite. This status monitor does not write output to disk.

48. Finally, we note that the gslite source code contains functions and methods that are never executed, and which appear to constitute vestigial or uncalled code. Stroz Friedberg

inspected such code but found no control flow that would lead to the execution of such code areas.

## ***B. Frame Parsing***

49. Following capture of the data by Kismet, gslite uses a Dot11Frame object to represent the structure of an 802.11 frame in memory, prior to writing the frame to disk. The gslite program processes these Kismet packets by removing the Kismet header, and then processing the underlying raw data, which is an 802.11 frame.

50. "Parsing" a property of an 802.11 frame results in its value being assigned to a property of Dot11Frame object, making it readily accessible for further analysis by gslite without additional decoding. Some 802.11 frame fields are analyzed by gslite and never assigned to a specific property of the Dot11Frame field object. Only some 802.11 frame fields are assigned to properties of Dot11Frame objects in their parsed form by gslite prior to being written to disk; others are stored in memory in a property field named "raw" and are written to disk without being further processed. By default, in the case of encrypted 802.11 Data frames, the frame's body, which was temporarily stored in the Dot11Frame's raw field, is cleared from memory and never written to disk.

51. Specifically, gslite parses all available 802.11 frame header information and stores those properties in memory in a Dot11MacHeader object. The remaining frame data, the body, is stored in its raw form in the raw property field of a Dot11FrameBody object. A Dot11MacHeader object is a representation of the 802.11 frame header in the memory of a computer. Similarly, a Dot11FrameBody is a representation of the body or payload of an 802.11 frame body.

52. The Dot11MacHeader's properties and the Dot11FrameBody object may be further analyzed or parsed depending on the type of frame. Dot11FrameBody objects contain ManagementFrameBody and ControlFrameBody objects to represent metadata specific to Management and Control frames respectively:

- a. Control frames undergo the least additional analysis as they contain comparatively less data than other frame types. Only the subtype information from an 802.11 Control frame's Frame Control field will be parsed and stored in memory as its own parsed property.
- b. Management frames, which contain the administrative information necessary to manage wireless transmissions, undergo both additional analysis, and parsing. Management frames' Frame Control properties are analyzed to determine the values of the To DS and From DS fields, which indicate the number of MAC addresses within the frame; however, these values are not stored in their own property fields in memory. Furthermore, Management frames' bodies are parsed and stored as a series of Information Elements in the ManagementFrameBody's collection of InformationElement objects. Included in the Information Elements properties is the SSID. The gslite program parses and stores the SSID information for all wireless networks, whether the SSID is broadcast or not. Any extra data stored in the ManagementFrameBody is stored in the "extra" property. Once this process is complete, the raw property of the Dot11FrameBody object is then cleared for Management Frames.

53. Although Data frame header information is further analyzed during the parsing process, Data frame bodies are not parsed. Specifically, gslite analyzes a Data frame's Frame Control field to determine the values of the To DS and From DS fields contained therein; however, these values are not parsed or stored in their own properties in memory.

54. In summary, the parsing function of the gslite program does the following:

- a. All 802.11 frames have all of their available 802.11 frame header information parsed and stored in properties of a Dot11MacHeader object in memory, regardless of frame type. A frame's body will be stored as raw data in a Dot11FrameBody's raw property, and this raw data may be further parsed if the frame is a Management Frame. The frame type information from a frame's Frame Control field is parsed and stored in memory as its own value, regardless of frame type.
- b. If the frame is a Control frame, the subtype information from the Frame Control field will be parsed and stored in memory as its own value. No additional parsing is performed on Control frames.
- c. If the frame is a Management frame, the To DS and From DS fields from the Frame Control field are analyzed, but are not parsed and stored in memory as their own properties. Management frame bodies are parsed and stored as a series of Information Elements in ManagementFrameBody's collection of InformationElement objects (which is in the Dot11Frame's Dot11FrameBody object). Any extra data in the body is stored in the ManagementFrameBody's "extra" property, and the "raw" property of the Dot11FrameBody object is cleared.
- d. If the frame is a Data frame, the To DS and From DS fields from the Frame Control field are analyzed, but are not parsed and stored in memory as their own properties. Data frame bodies are not parsed. As discussed more fully below, the body of a Data frame is discarded if the Protected Frame bit is set to "true", which indicates the frame is encrypted; otherwise, the body is written as unparsed data to disk.

### **C. Default Settings Governing Discard of Data and Writing to Disk**

55. After gsliite's program logic parses each 802.11 frame according to its type, a Dot11Frame object exists with all available frame properties parsed and stored in the appropriate property fields. At this point in the execution of the program, the program's settings are checked to determine whether or not to retain the current frame data in whole or in part.

56. By default, gsliite records all wireless frame data, except for the bodies of Data frames from encrypted wireless networks. The code governing whether data elements of a frame should be retained or discarded occurs in the file "packetparserimpl.cc." Four variables, or flags, are assigned default Boolean values to establish the program's default behavior regarding what to discard from memory and what to retain. In particular, the default settings, as shown below, are set to discard the bodies of encrypted frames<sup>3</sup> and to retain everything else (packetparserimpl.cc lines 14-21):

```
DEFINE_bool(discard_encrypted_body, true,
    "Discard bodies of encrypted 802.11 frames");
DEFINE_bool(discard_control_frame, false,
    "Discard 802.11 control frames");
DEFINE_bool(discard_data_frame, false,
    "Discard all 802.11 data frames");
DEFINE_bool(discard_management_frame, false,
    "Discard all 802.11 management frames");
```

<sup>3</sup>Although a Management frame of the subtype Authentication would have its encryption flag set to "true," the sequence of the execution path causes such Management frame bodies to be stored in the "extra" property and written to disk. Management frames do not contain user content.



57. The same file, `packetparserimpl.cc`, contains the code that checks each wireless frame processed and determines whether or not to retain it in whole or in part, based upon the Boolean values of the flags defined above. The program checks to see whether the "discard\_encrypted\_body" flag is set to "true", which is the default setting. If so, `gslite` checks the frame being parsed to see whether its encryption flag is set to "true." If both checks return "true" then the frame is encrypted and the program discards the encrypted frame's body. The frame body is cleared, using the accessor method `clear_body()`.

```
if (FLAGS_discard_encrypted_body && PacketUtil::IsEncrypted(f)) {
    // Discard just the body of encrypted frames
    f->clear_body();
}
```

Subsequently, when the remainder of the frame is written to disk, its body is not recorded.

58. The program checks the type of the frame being parsed (that is, whether it is a Control, Data, or Management frame) and then checks the value of the corresponding Boolean flag from among the discard flags above. If it is "true", the discard flag of the current frame object is set using the `Dot11Frame` accessor method `set_discard(true)`.

```
switch (PacketUtil::Type(f)) {
case Dot11FrameBody::CONTROL:
    if (FLAGS_discard_control_frame)
        f->set_discard(true);
    break;
case Dot11FrameBody::DATA:
    if (FLAGS_discard_data_frame)
        f->set_discard(true);
    break;
case Dot11FrameBody::MANAGEMENT:
    if (FLAGS_discard_management_frame)
        f->set_discard(true);
    break;
default:
    break;
}
```

59. At a subsequent point in program execution when a parsed frame is to be written to disk, the discard flag of the frame object is checked: if the flag is set to "true", the frame is not written to disk (`scanner.cc` lines 105-111):

```
void WifiScanner::TryLog(Dot11Frame * frm) {
    if (is_logging_ &&
        logger_ &&
        !frm->discard() &&
        !logger_>Write(frm))
        LOG(ERROR) << "Error writing to log";
}
```

#### **D. GPS Interpolation**

60. The onboard GPS system provides geolocation coordinates at some rate slower than the rate at which wireless frames can be received. Accordingly, `gslite` interpolates the position at which each wireless frame was received and associates the interpolated position with the frame object. Stroz Friedberg's review of source code relating to GPS coordinate interpolation found no code execution paths that would affect the wireless data written to disk by `gslite`.

### ***E. Command Line Arguments in Configuration Files***

61. The Boolean flag definitions set forth in section C above provide the default program behavior. However, the flags can be superseded by command line arguments defined in accordance with Google's coding standards. The first line of code executed by gslite processes any and all command line arguments (see gslite.cc lines 12 and 128-129, below). It is our understanding from Google that InitGoogle(), a method defined outside the scope of the provided source code, sets the values of program variables using the command line arguments. The Google standards for using command line flags is documented at <http://google-gflags.googlecode.com/svn/trunk/doc/gflags.html>.

```
#include "base/commandlineflags.h"
...
int main(int argc, char** argv) {
    InitGoogle(argv[0], &argc, &argv, true);
```

62. Command line arguments will supersede the default values for the discard and encryption flags discussed above and change the behavior of gslite. Since the flag "discard\_data\_frame" is false by default, gslite will discard entire Data frames if and only if the flag "discard\_data\_frame" is run on the command line at the time of program execution (or until such time as the default behavior is revised in source code).

### **V. Conclusion**

63. Gslite is an executable program that captures, parses, and writes to disk 802.11 wireless frame data. In particular, it parses all frame header data and associates it with its GPS coordinates for easy storage and use in mapping network locations. The program does not analyze or parse the body of Data frames, which contain user content. The data in the Data frame body passes through memory and is written to disk in unparsed format if the frame is sent over an unencrypted wireless network, and is discarded if the frame is sent over an encrypted network.

## APPENDIX A

### INVENTORY OF REVIEWED SOURCE CODE FILES AND SHELL SCRIPTS

Stroz Friedberg reviewed the following provided C++ source code, configuration files, and shell scripts as part of its static source code analysis. The dates of last modification are derived from the compressed tar files in which the source code was provided and are believed to correspond to the dates of modification of official, checked-in source code.

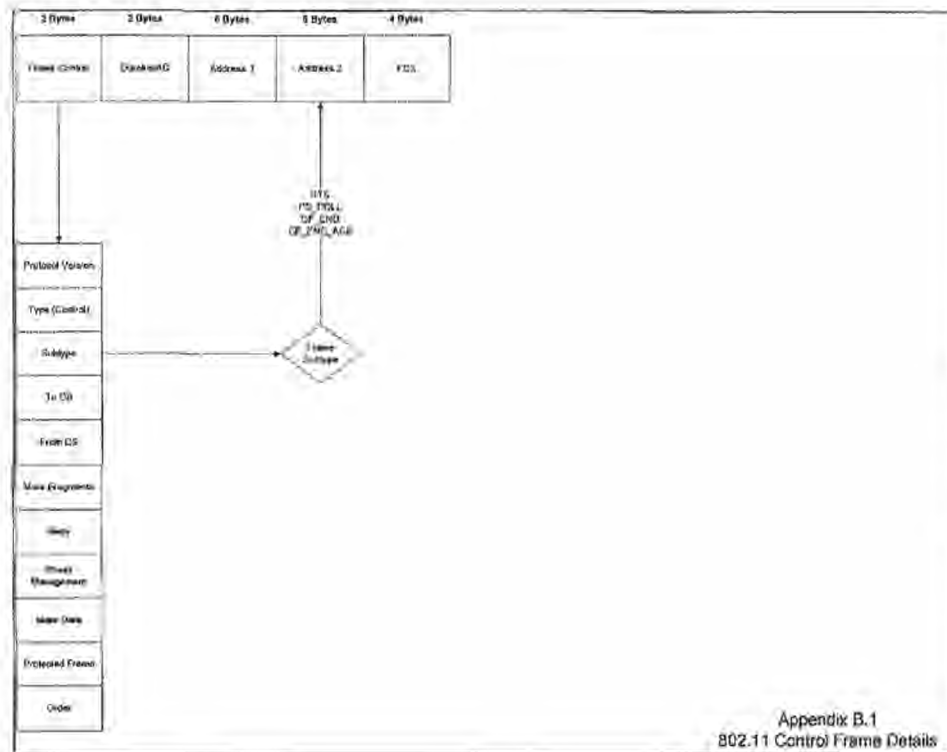
File Name	Last Written On	SHA-1 Hash Value
<b>gstumbler Source Code</b> Provided as <b>gstumbler-src.tgz</b> on 5/20/2010		
BUILD	7/1/2009	7de19d35307cfdc9fc8c03c9d8d44aee3cebcbaa
gps_messages.h	3/31/2010	aa9ce1443f3e1352056751cdc3ca8d35705cbf11
gps-interpolator.cc	11/7/2007	37001680b7e4acd0410fd890523fa911371cd163
gps-interpolator.h	4/30/2008	688d310771e86e2ecc92c7069059bda2e378d1d8
gps-interpolator_test.cc	2/2/2010	21e241b6c0b0ae65f2d395f38d5541d0e12b3ed8
gps-ipc.cc	3/31/2010	2413c0538add232332fa25ba1498274f54e2d76f
gps-ipc.h	3/31/2010	175193adb5118594e8f644c9b9bb8a9920476d8a
gps-ipc_test.cc	3/31/2010	3ea76455f6d12391c6e60ad9d8b0fe9bffb0db4
gsllite.cc	3/31/2010	796c67b420fd5f0a1bc65c42c07d08256686d3
gstumbler.cc	4/30/2008	2104989fde44b9c53acbf5bc6857ee8f11c2594e
gstumbler-run.sh	3/5/2007	e5045fac3b9e5de3ce36b3b797e504a9c741254a
kismetconnection.cc	6/19/2009	4b3cb2dcfe03c53bdf3f46088039c1105d29fe3
kismetconnection.h	6/19/2009	cac68ca54136cc1bct3a84f9a54a25b4939f2a7f
logger.cc	11/7/2007	03f2733398191d36fae6297564b455086bdfda83
logger.h	11/7/2007	83df12f13e50f5e070af8f4ac1c032ca6a2f8662
monitor.cc	10/31/2006	7b5381eb9adeb12e09589f84e817f170bc783ade
monitor.h	10/31/2006	64870c0f3df0b169ef352b0c3f920bd48f6073c
packet.proto	3/31/2010	872e43bb2477b3d50dfdd34f68adad7290f49f6c
packetparser.cc	10/31/2006	142687c8f5bef580ce46476eb840e0022280d969
packetparser.h	7/1/2009	3855b17808778d752824ea6a2efbe875307933ac
packetparser_test.cc	2/2/2010	dc795a3e99ec890db87d1e97ac835ec3f74a3f7b
packetparserimpl.cc	10/31/2006	ec094b96ab14ba7bf251160ad6d3285d41a3a714
packetparserimpl.h	10/31/2006	d8f5c40b3954133c8be46e6cabf9f23f91de6ecc
packetsource.cc	10/31/2006	bfe8dec9aa9d4a4095c0ad34c9f103b7344154d5
packetsource.h	3/4/2010	89f2b4ffa32e925e58bdf0f58097cf5bd7ce0ed9
packetsourceimpl.cc	12/16/2009	75828b368c1682ebac547c1193e9d3fbcc27f54a
packetsourceimpl.h	7/1/2009	bff09f7f55cdd080eaf1d9057a8a33c1d9cbb8f8
packetutil.h	1/28/2008	8dedee1c5b43811bd7a16ea9b5afc58b69adf2f2
resources/drive_status.tpl	10/18/2007	065c489ee01d5de2f185f92829fceebed58359e9
scanner.cc	3/31/2010	33d4a92a87a679faf0932e492f6e6cf32a9534a
scanner.h	3/31/2010	4a869a3f54a4f2662c09b8fd90e4e14bf631cb83
scanner_test.cc	2/2/2010	7a8004d0c19cc1337ca9cb888bd3f7830a26413b
<b>Configuration files and shell scripts -- most recent versions</b> Provided as <b>gstumbler-config.tgz</b> on 5/20/2010		
config_interfaces.sh	5/18/2010	51c00340e9744dda850ca0ee546bccc067327caa
kismet_drone.conf.template	5/18/2010	f5bd93b3fc1ba8ada0827cc041c6ca5c24aab99c



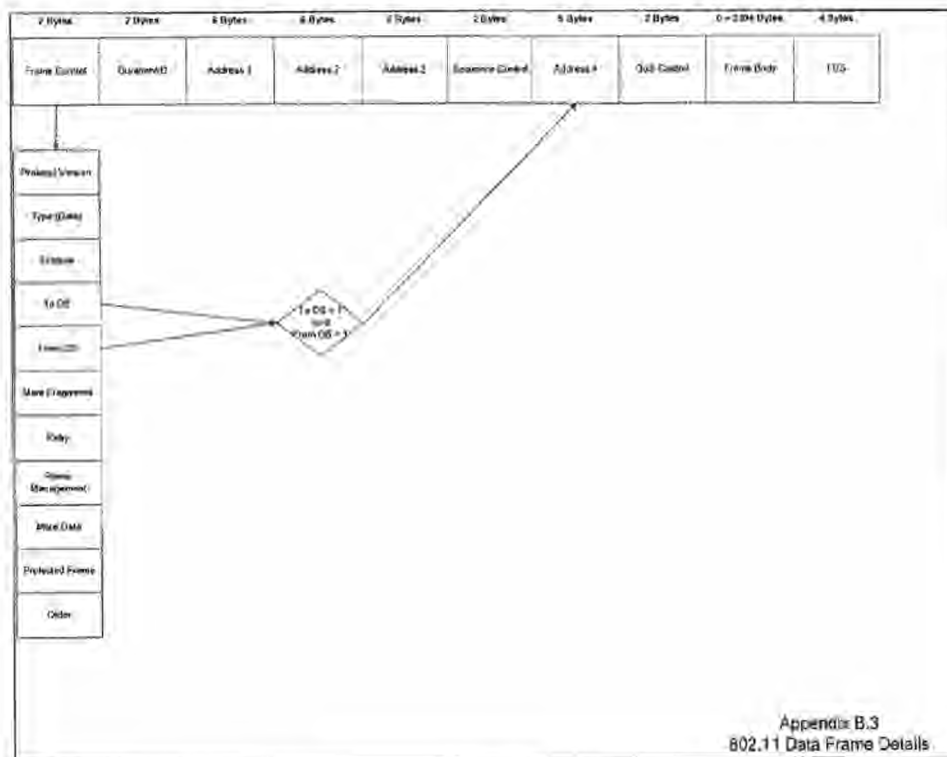
run_gstumbler.template	5/18/2010	7b3aacb15f8b878b8bd91d34242c6b4a1e958691
run_kismet	5/18/2010	7c8b2b13061b6cb8280258556910d56b93848a20
<b>Configuration files and shell scripts -- historical versions</b>		
<b>Provided as gstumbler-scripts2.tgz on 5/26/2010</b>		
config_interfaces.sh#1	5/26/2010	7b85ea7c7babd7a7115f0caa1fc1e3a2814f8d75
config_interfaces.sh#2	5/26/2010	faeeeb1ae425597af82acebdedccc2c972080b10
config_interfaces.sh#3	5/26/2010	5818de44b2c167116958e7bd35240b11f3186953
config_interfaces.sh#4	5/26/2010	1c5ee14d002970d532ec55cee09962959b78d28b
run_gstumbler.template#1	5/26/2010	9a718b8727a2c590e670fc08ea27fa4818309253
run_gstumbler.template#2	5/26/2010	414ca3f5d2175eecd11c104a8aba702cce34778
run_kismet#1	5/26/2010	27df00844852cd7e0070d82324ab5cc2fb81881c
<b>Supporting library for managing record writing</b>		
<b>Provided as bulkstorage.tgz on 5/26/2010</b>		
bulkstorageblock.h	11/1/2008	d7240f808766bd718e80f11293dcaba95f50af18
bulkstoragewriter.cc	3/12/2007	e361e6c9d16cc64af15bb3df6a6c1dd58e049b6f
bulkstoragewriter.h	3/12/2007	d0dad037253f4f83a9107c7ea004c8d8e28f78d1
bulkstoragewritermanaged.cc	3/4/2010	bab20ee94c25d62c2d8a18259915bf0906d68115
bulkstoragewritermanaged.h	3/4/2010	1d8b67f468f0b3d7dbe4f609548261b37fed4eb0
disk_write_methods.cc	3/12/2007	134aea15d93f667a322e7c70c7b89609755e2052
disk_write_methods.h	12/29/2006	4609dcf39b55cc2e111f338b7dbc4a3ca1891109
performancemonitor.cc	8/10/2007	14aece5bd4bcb520e654ab0d9802c560c2e1c09
performancemonitor.h	11/29/2006	b8c37eb8a427fdd72f707985661a71641c7436ec
sectensecmstats.cc	11/29/2006	34d884b123216a4fb5bd640bf51d2e8f2ad42ef1
sectensecmstats.h	6/22/2009	38c8bf84879ecdade44a31642b5aba0e30e8cccd

## APPENDIX B

### 802.11 FRAME ELEMENTS







## **APPENDIX C**

### **THE GSTUMBLER DOT11FRAME PROTOCOL BUFFER AND SUMMARY OF RECORDED CONTENT**

C-1. Google source code employs a serialization format, accomplished through the use of objects developed at Google called Protocol Buffers, which are used to exchange and write structured data. Protocol Buffers take an object representing a complex data structure and transform that structured object into a bitstream, suitable for transmission or writing to disk, through a transformation called serialization. The source code for protocol buffers was released under an open source license by Google in 2008. An overview of documentation regarding protocol buffers is available at (<http://code.google.com/apis/protocolbuffers/docs/overview.html>).

C-2. Each type of object to be serialized is specified as a Protocol Buffer "message," which establishes the structure of each object type. In the gstumbler project source code, Protocol Buffers are declared in the file packet.proto. The protocol buffer message of central importance to gslite's functionality is the Dot11Frame object, a message that is a structured representation of a single 802.11 wireless frame. The Dot11Frame object contains multiple other protocol buffer messages, also defined in packet.proto, that represent various components and types of wireless frames.

C-3. Protocol buffers provide accessor functions to set and retrieve the values of fielded data within a message. Standard accessor functions include get\_<fieldname>, set\_<fieldname>, and clear\_<fieldname>, where <fieldname> is one of the defined data elements within the message. As discussed in paragraphs 57 and 58 of this report, the Dot11Frame accessor methods clear\_body() and set\_discard(true) will be called if certain flags and conditions are true. These methods serve, respectively, to clear only the content of the Dot11Frame's Body field and to set the Discard Boolean flag of a Dot11Frame message to true. These two methods are the means by which a frame is written to disk without its payload or not at all.

C-4. The following tables summarize the properties within each of the protocol buffer messages defined in packet.proto.

<b>Dot11Frame Object</b>	
<b>Property</b>	<b>Description</b>
Raw	A buffer used to store the unprocessed data; this buffer contains the raw frame data parsed throughout frame processing and is cleared prior to the data being written to disk.
Header	A Dot11MacHeader object in the protocol buffer message format described below.
Body	A Dot11FrameBody object in the protocol buffer message format described below.
Position	A cityblock.PositionInfo object containing GPS coordinates.
PositionComment	An optional string.
TimeRecvd	The time the frame arrived for processing.
TimeSent	The estimated time the frame was transmitted.
KismetMetadata	A KismetMetadata object, described below, containing per-packet information including 802.11 channel, signal quality, and frame length.
Discard	A boolean flag that indicates whether or not the entire frame – metadata and body – should be written to disk.

Dot11MacHeader	
Property	Description
Raw	The raw data buffer containing the data that is processed and stored in the header's fields.
FrameControl	A thirty-two bit integer used to store the sixteen bit Frame Control field in an 802.11 frame.
DurationOrId	A thirty-two bit integer used to store the sixteen bit field in position bytes 2 to 3 in an 802.11 frame. These sixteen bits are either the duration or id depending on the type and subtype of the frame.
Address1	The first Media Access Control (MAC) address in an 802.11 frame. A MAC address is a six byte hexadecimal address specifying a network device.
Address2	The second MAC address in an 802.11 frame.
Address3	The third MAC address in an 802.11 frame.
SequenceControl	The sixteen bit sequence control number present in data and management frames. Data may be fragmented for transmission or re-transmission. If the data is fragmented, this number is used to determine where in sequence a fragment fits. This field is zero for the first or only fragment of data, and incremented for each successive fragment sent.
Address4	The fourth MAC address in an 802.11 frame.
QoSControl	Sixteen bits of quality of service related information and policies sent by hardware supporting quality of service.

Dot11FrameBody	
Property	Description
Raw	The raw data buffer containing the data that is processed and stored in the body's fields.
FrameType	An enumerated type that specifies if a frame is: a Management frame (0); a Control frame (1); a Data frame (2); a Reserved type frame (3); or if there is no frame type detected (9999).
Ctrl	An optional ControlFrameBody object, defined below.
Mgmt	An optional ManagementFrameBody object, defined below.

ControlFrameBody	
Property	Description
Subtype	An enumerated type specifying the subtype of a Control frame. Its potential values are: PS_POLL (10); RTS (11); CTS (12); ACK (13); CF_END (14); CF_END_ACK (15); and NO_CTRL_SUBTYPE (9999).

ManagementFrameBody	
Property	Description
Subtype	An enumerated type specifying the subtype of a Management frame. Its potential values are: ASSOC_REQ (0); ASSOC_RESP (1); REASSOC_REQ (2); REASSOC_RESP (3); PROBE_REQ (4); PROBE_RESP (5); BEACON (8); ATIM (9); DISASSOC (10); AUTH (11); DEAUTH (12); and NO_MGMT_SUBTYPE (9999).
AuthAlgorithm	A thirty-two bit integer that is not set in the code reviewed.
AuthTransaction	A thirty-two bit integer that is not set in the code reviewed.
BeaconInterval	A thirty-two bit integer that is used to store the sixteen bit value of the number of time units between target beacon transmission times.
Capability	A thirty-two bit integer that is used to store the sixteen bit series of flags outlining the functionality of the transmitter.

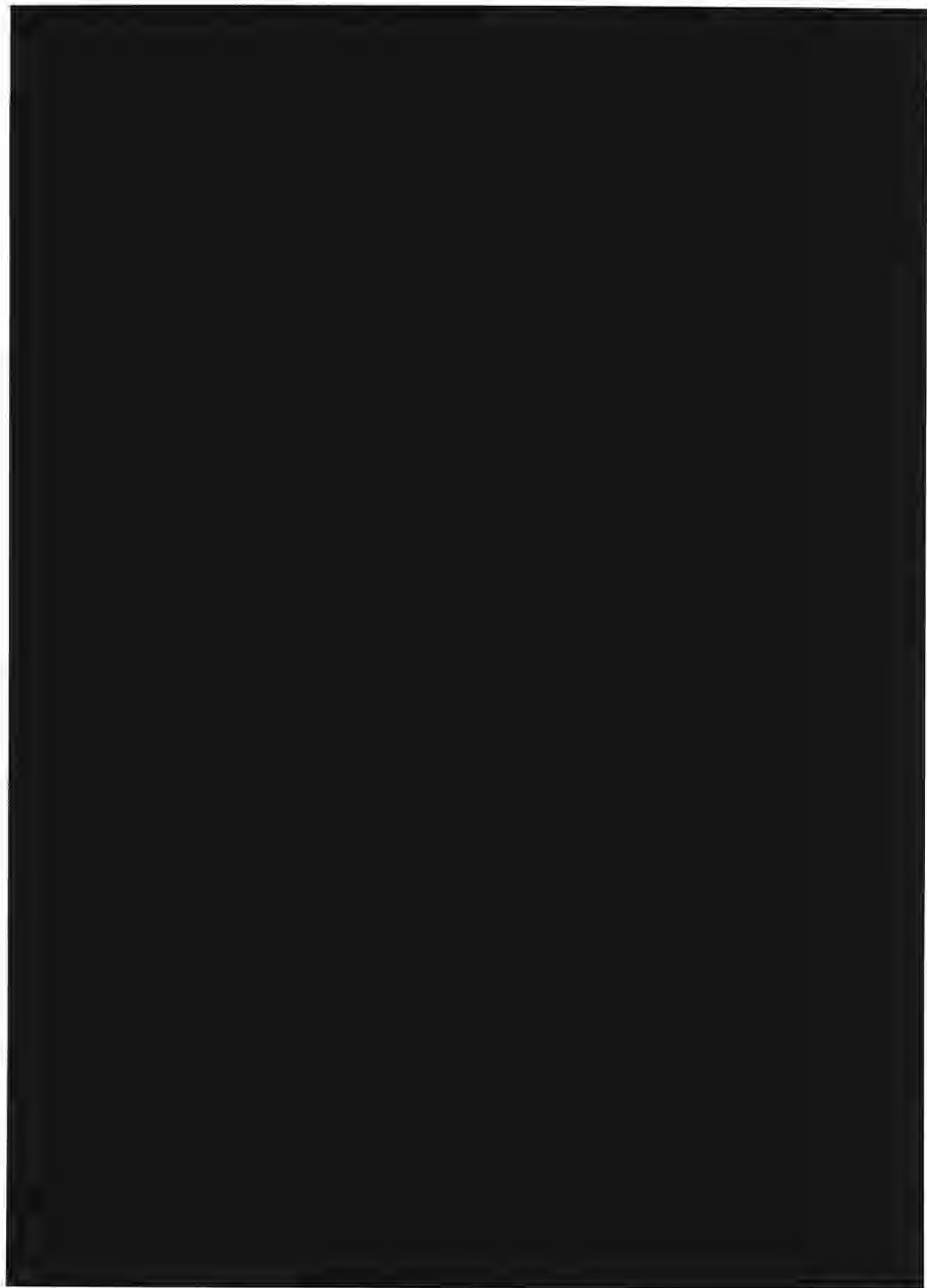
CurrentBSSID	A sixty-four bit integer that is used to store the forty-eight bit MAC address of the access point with which the transmitter is currently associated with.
ListenInterval	A thirty-two bit integer used to store the sixteen bit value of how often a receiver in power saver mode wakes to listen to Beacon management frames.
ReasonCode	A thirty-two bit integer that is not set in the code reviewed.
AssocID	A thirty-two bit integer that is used to store the sixteen bit value assigned by an access point during the association process.
StatusCode	A thirty-two bit integer that is used to store the value used in a response management frame to indicate the success or failure of a requested operation.
Timestamp	A sixty-four bit integer used to store the value of the timing synchronization function timer of a frame's source.
IEs	A collection of Information Elements, or key-value pairs regarding a transmitter.
SSID	A string containing the name of the access point.
Channel	A thirty-two bit integer used to store the channel on which a frame was sent.

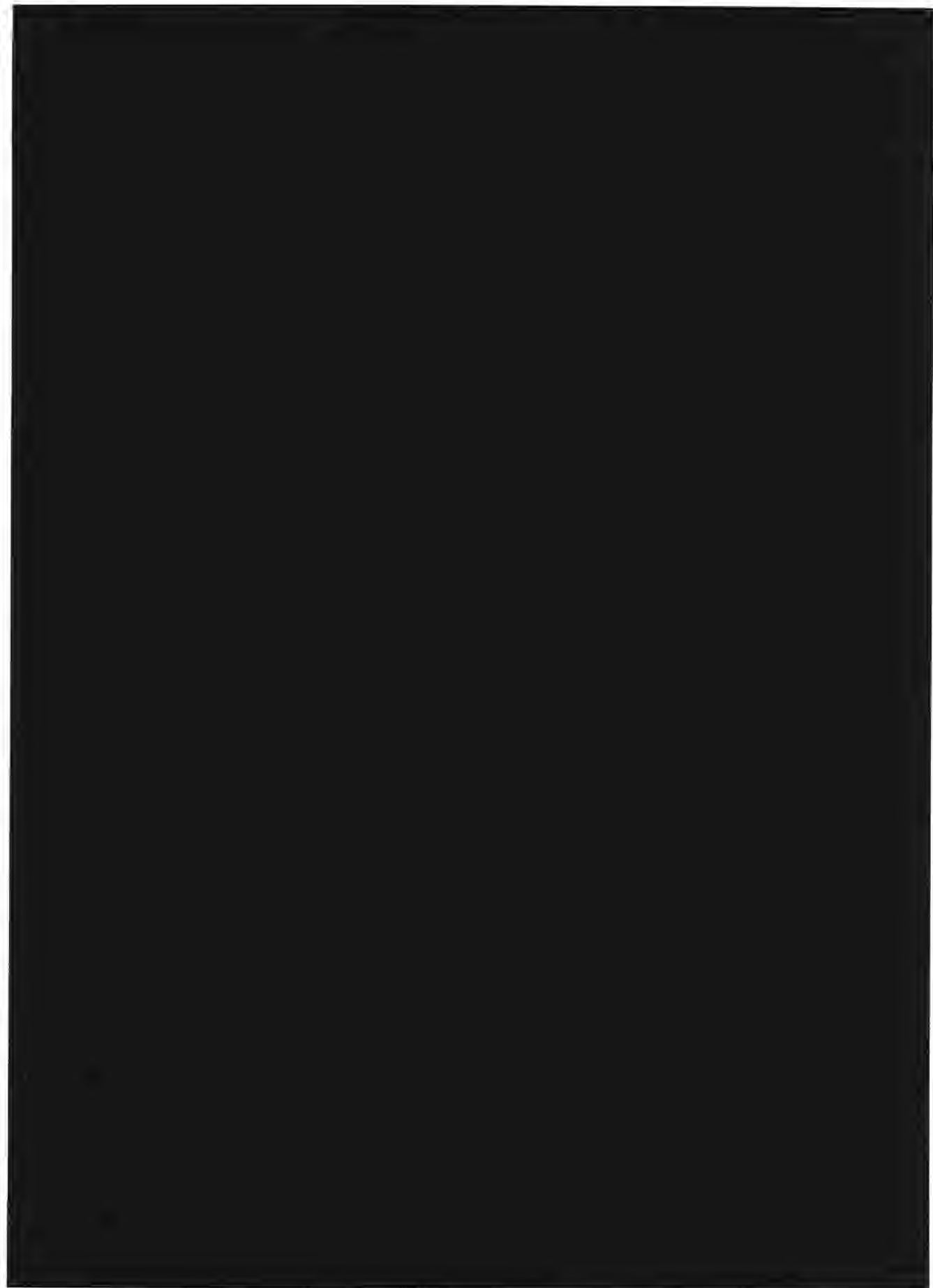
KismetMetadata	
Property	Description
hdrlen	A thirty-two bit integer used to store the length of the Kismet header.
drone_ver	A thirty-two bit integer used to store the sixteen bit value of the version of the Kismet drone.
datalen	A thirty-two bit integer used to store the length of the data captured by Kismet.
caplen	A thirty-two bit integer used to store the length of the data originally captured by Kismet.
tv_sec	A sixty-four bit integer storing a timestamp in seconds.
tv_usec	A sixty-four bit integer storing a timestamp in microseconds.
quality	A thirty-two bit integer used to store the sixteen bit value signal quality.
signal	A thirty-two bit integer used to store the sixteen bit value signal strength.
noise	A thirty-two bit integer used to store the sixteen bit value signal noise level.
error	A thirty-two bit integer used to store the eight bit value whether the capture source told Kismet the frame was bad.
channel	A thirty-two bit integer used to store the eight bit value of the hardware channel that received the frame.
carrier	A thirty-two bit integer used to store the eight bit value of the signal carrier.
encoding	A thirty-two bit integer used to store the eight bit value of the signal encoding.
datarate	A thirty-two bit integer used to store the value of the data rate, which is in units of 100 kbps.
adapter	A thirty-two bit integer used to store the mapped value of an adapter name.

## **Appendix B**









## Appendix C

**Organization Information:**

Google Inc.  
1600 Amphitheatre Parkway  
Mountain View, California- 94043  
Phone: (650) 253-4000  
Fax: (650) 618-1499  
<http://www.google.com>

**Contact Information:**

Contact Office: Legal Department  
Contact Name: ,  
Contact Phone: (650) 253-4000  
Contact Fax: (650) 618-1499  
Contact Email: [privacymatters@google.com](mailto:privacymatters@google.com)

**Corporate Officer Information:**

Corporate Officer: Jane Horvath , Global Privacy Counsel  
Phone: (202) 346-1294  
Fax: (650) 618-1499  
Email: [JaneHorvath@google.com](mailto:JaneHorvath@google.com)

**Safe Harbor Information:**

Signed up to Safe Harbor: 10/15/2005  
Next Certification: 10/15/2011

**Personal Information Received from the EU:**

Google Inc., and other companies within the Google Inc. corporate group, collect personal information in relation to natural persons from within member states to the European Union ("EU data subjects") as result of: 1) the use and operation by Google Inc. and its group members of internet domains which are registered in member states of the European Union from which Google Inc. and its group members carry on their business and supply services to EU data subjects; and 2) the distribution, within member states of the European Union, by Google Inc. and its group members (and other third parties authorised to do so by Google Inc. and its group members) of applications and products to EU data subjects; and 3) the supply of goods and/or services to Google Inc. and its group members by companies and businesses located in member states of European Union (which may in some cases involve the supply or exchange of personal information in relation to EU data subjects). Personal information collected under (1) and (2) is held and processed by Google Inc. and its group members for differing purposes depending upon the particular service or product being provided. These purposes may include any of the following: sales and marketing to such consumers and/or businesses, contract negotiation, effecting transactions with such consumers and/or businesses, supplying services and/or products to such consumers and/or businesses, operating, developing and improving our services and products, personalising our services and products, financial processing and management, fraud detection and prevention, compliance with governmental, legislative and regulatory bodies, customer support and/or customer relationship management. Personal information collected under (3) is held and processed by Google Inc. and its group members for differing purposes depending upon the nature of the supply of goods and/or services. These purposes may include any of the following: contract negotiation, effecting transactions with such individuals and/or businesses, financial management and/or supplier relationship management, fraud detection and prevention, and compliance with governmental, legislative and regulatory bodies.

Privacy Policy Effective: 10/3/2010

Location: [google.com/intl/en/privacypolicy.html](http://google.com/intl/en/privacypolicy.html)

Regulated By: Federal Trade Commission

Privacy Programs:  
NONE

Verification: In-house

Dispute Resolution:

Federal Trade Commission and cooperation with EU data protection authorities pursuant to the Safe Harbor certification

Personal Data Covered: off-line, on-line, manually processed, human resources data

Human Resource Data Covered: Yes

Do you agree to cooperate and comply with the European Data Protection Authorities? Yes

**EU/EEA Countries From Which Personal Information Is Received:**

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Slovakia, Spain, Sweden, Switzerland, United Kingdom

Industry Sectors:  
Information Services - (INF)

Certification Status: Current

Compliance Status:

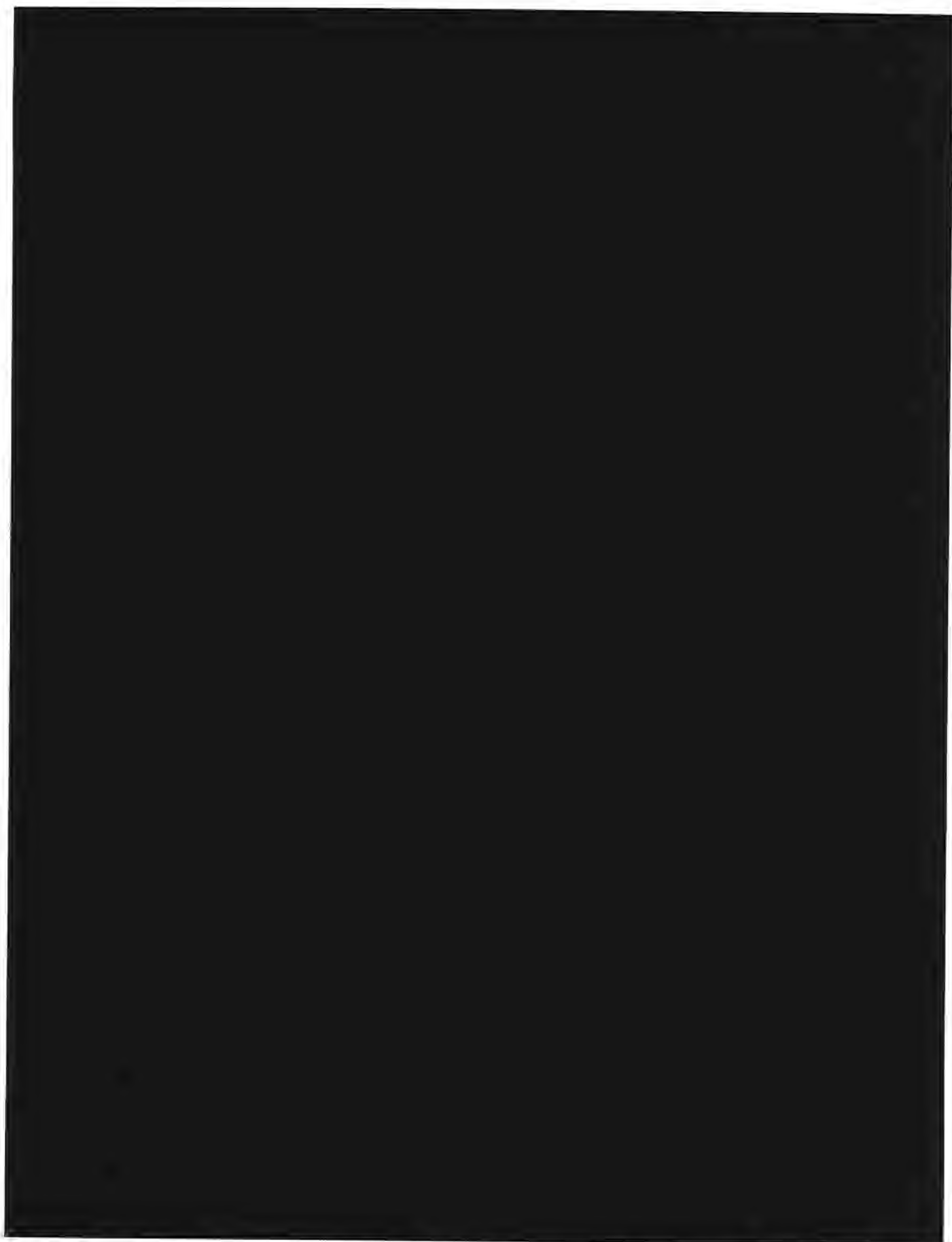
## Appendix D

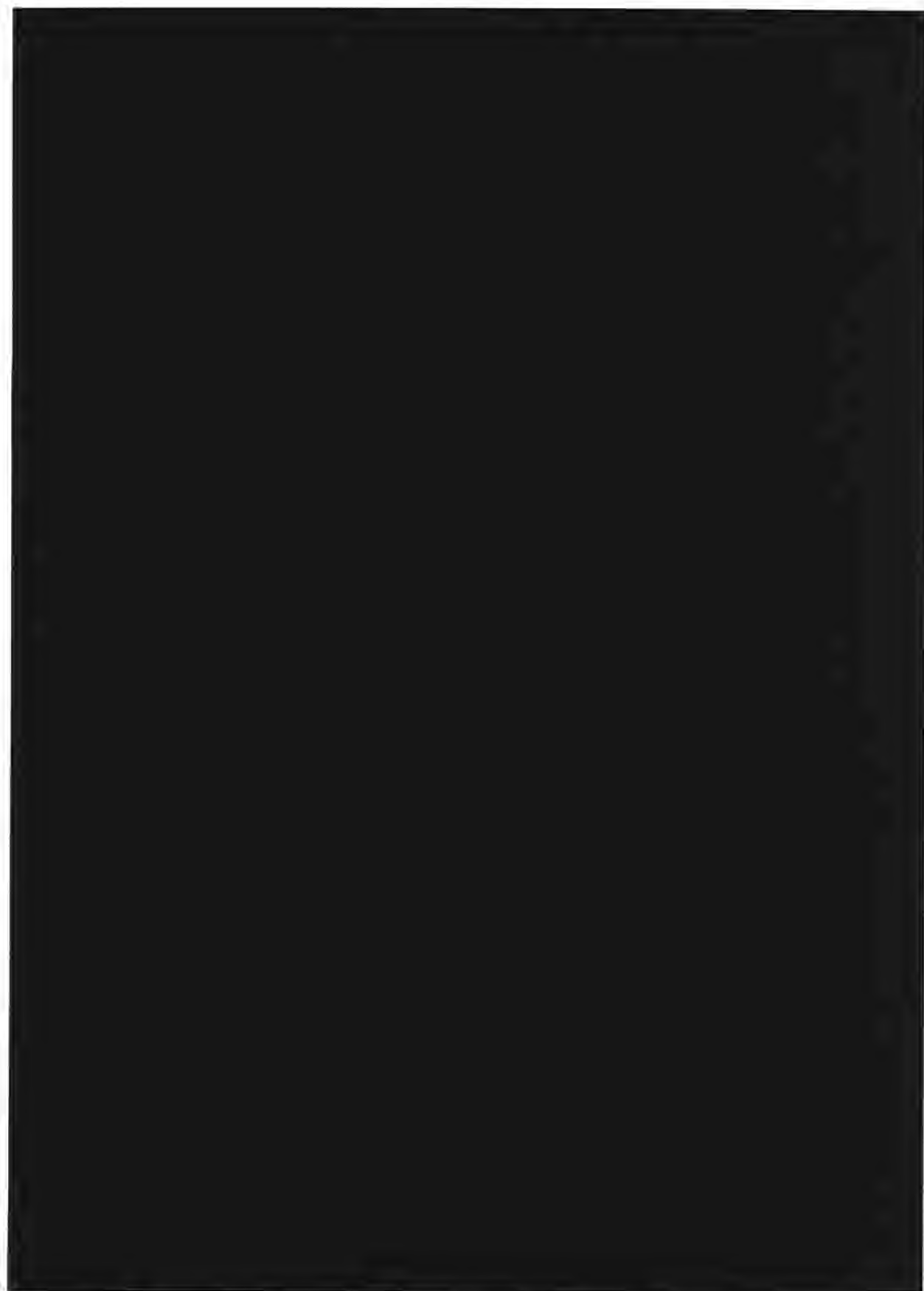




## Appendix E









1. The first part of the document discusses the importance of maintaining accurate records of all transactions and activities. It emphasizes that proper record-keeping is essential for transparency and accountability, particularly in financial matters. The text outlines various methods for organizing and storing data, including digital databases and physical filing systems. It also mentions the need for regular audits and reviews to ensure the integrity of the information.

2. The second section focuses on the role of communication in achieving organizational goals. It highlights the importance of clear and concise communication, both internally and externally. The text provides guidelines for effective communication, such as using appropriate language, listening actively, and providing feedback. It also discusses the benefits of open communication and how it can foster a collaborative work environment.

3. The third part of the document addresses the issue of time management. It recognizes that time is a valuable resource and that efficient use of time is crucial for productivity. The text offers several strategies for managing time effectively, including prioritizing tasks, setting deadlines, and avoiding distractions. It also mentions the importance of taking breaks and maintaining a healthy work-life balance.

4. The final section discusses the importance of continuous learning and professional development. It emphasizes that individuals should strive to stay updated with the latest trends and technologies in their field. The text suggests various ways to acquire new skills, such as attending workshops, conferences, and taking courses. It also mentions the importance of seeking mentorship and networking with professionals in the industry.

the 'information' and 'communication' fields. The 'information' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'communication' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of communication, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information science' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information studies' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information technology' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information systems' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information management' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information policy' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information law' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)

The 'information ethics' field is defined as:

...the study of the nature, creation, organisation, storage, retrieval, dissemination and use of information, and the social, cultural, economic and political contexts in which these activities take place. (p. 1)







## Appendix F



The first part of the paper discusses the importance of the research and the objectives of the study. It then presents a literature review of the existing research on the topic. The methodology section describes the research design and the data collection process. The results section presents the findings of the study, and the conclusion section summarizes the main points and provides recommendations for future research.

The study was conducted in a laboratory setting, and the participants were recruited from a local university. The data was collected using a series of questionnaires and interviews. The results of the study show that there is a significant relationship between the variables studied. The findings suggest that the research has practical implications for the field.

The study was limited by the sample size and the laboratory setting. Future research should aim to replicate the study in a more naturalistic setting and with a larger sample size. The results of the study provide a foundation for further research in this area.



the 1990s, the number of people in the UK who are employed in the public sector has increased by 1.5 million, from 2.5 million in 1980 to 4 million in 1995. The public sector has become a major employer in the UK, and its growth has been a key factor in the overall growth of the economy.

The public sector has also become a major provider of social services, and its growth has been a key factor in the overall growth of the economy. The public sector has become a major provider of social services, and its growth has been a key factor in the overall growth of the economy.

The public sector has also become a major provider of social services, and its growth has been a key factor in the overall growth of the economy. The public sector has become a major provider of social services, and its growth has been a key factor in the overall growth of the economy.

The public sector has also become a major provider of social services, and its growth has been a key factor in the overall growth of the economy. The public sector has become a major provider of social services, and its growth has been a key factor in the overall growth of the economy.

The public sector has also become a major provider of social services, and its growth has been a key factor in the overall growth of the economy. The public sector has become a major provider of social services, and its growth has been a key factor in the overall growth of the economy.

The public sector has also become a major provider of social services, and its growth has been a key factor in the overall growth of the economy. The public sector has become a major provider of social services, and its growth has been a key factor in the overall growth of the economy.

The public sector has also become a major provider of social services, and its growth has been a key factor in the overall growth of the economy. The public sector has become a major provider of social services, and its growth has been a key factor in the overall growth of the economy.

The public sector has also become a major provider of social services, and its growth has been a key factor in the overall growth of the economy. The public sector has become a major provider of social services, and its growth has been a key factor in the overall growth of the economy.



[The page contains a large, dense block of text that is mostly illegible due to extreme blurring and low contrast. The text appears to be organized into several paragraphs, but the specific words and sentences cannot be discerned.]







**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

December 14, 2010

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
236 Massachusetts Avenue, N.E., Suite 110  
Washington, DC 20002

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of Google's supplement to responses ("Supplement") to the November 3, 2010, letter to Google from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission (the "Bureau Letter") in the above-referenced matter.

As shown below, the Supplement contains information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential."<sup>1</sup>

Response to Request No. 9. The redacted portions of Google's Response to Request No. 9, including Document No. 11-6, contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company's internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Further, the Response includes trade secrets, including product design data, computer code, and descriptions of the processes by which Google creates and produces its products, which is highly

---

<sup>1</sup> 5 U.S.C. § 552(b)(4). See also 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

**Lampert, O'Connor & Johnston, P.C.**

December 14, 2010

Page 2

confidential and competitively sensitive information. Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

Except for Appendix A and Appendix C to Document 11-6, Google has not made the materials in Document 11-6 available to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and state attorneys general. Google believes it is necessary for the Commission to maintain the confidentiality of this information throughout the investigation and thereafter until it is destroyed.

Consistent with 47 C.F.R. § 0.459(d)(1), Google respectfully requests notification by the Commission if release of the redacted material in the Response is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
*Counsel to Google Inc.*

Enclosures

cc: Hillary DeNigro, Investigations and Hearings Division, Enforcement Bureau  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau



**SUPPLEMENT TO  
RESPONSES OF GOOGLE INC. TO LETTER OF INQUIRY  
FILE NO. EB-10-IH-4055**

The following supplement to responses is made subject to and without waiving the general objections stated in the Responses of Google Inc. ("Google") submitted December 10, 2010.

**REQUEST NO. 9:** Describe any remedial measures that have been implemented by Google to address interception or reception of communications as described in response to the preceding inquiries. Specifically, describe in detail the changes Google has made -- or intends to make -- to improve its internal privacy and security practices, including those mentioned in the October 22, 2010, Google blog posting.

**RESPONSE TO REQUEST NO. 9:**

As to the changes discussed in its October 22, 2010, blog post, Google provides a report of its process changes and improvements. This document is confidential and identified as Document 11-6.



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@iojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

December 20, 2010

**CONFIDENTIAL TREATMENT REQUESTED**

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W., Room TW-A325  
Washington, DC 20554

Attn: Mindy Littell  
Investigations and Hearings Division  
Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

Re: **Google Inc., File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google") hereby further supplements its responses, submitted December 10, 2010, to the letter dated November 3, 2010 from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission, which requests information about Google's collection of data from Wi-Fi networks in the United States.

Kindly contact me should there be any questions regarding this submission.

Respectfully submitted,



E. Ashton Johnston  
*Counsel for Google Inc.*

Enclosures

cc: Hillary DeNigro, Investigations and Hearings Division, Enforcement Bureau  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau





**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@iojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

December 20, 2010

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
236 Massachusetts Avenue, N.E., Suite 110  
Washington, DC 20002

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of Google's second supplement to responses ("Second Supplement") to the November 3, 2010, letter to Google from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission (the "Bureau Letter") in the above-referenced matter.

The Second Supplement contains information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential,"<sup>1</sup> and Exemption 7(C), which provides a statutory basis for withholding from public inspection information compiled for law enforcement purposes and that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."<sup>2</sup> We enclose herewith both a complete, unredacted copy of the Second Supplement, to be treated as confidential, and a separate copy of the Second Supplement marking specific portions thereof as Redacted.

Response to Request Nos. 5 and 10. The redacted portions of Google's Second Supplement contain sensitive, personal information that relates to Google's business, "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not

---

<sup>1</sup> 5 U.S.C. § 552(b)(4). *See also* 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

<sup>2</sup> 5 U.S.C. § 552(b)(7)(C). *See also* 47 C.F.R. 0.457(g)(3).

**Lampert, O'Connor & Johnston, P.C.**

December 20, 2010

Page 2

routinely disclose such material to the public or to third parties, and has established procedures to protect such highly confidential information internally. *See* 47 C.F.R. § 0.459(a)(4). The redacted portions of the Second Supplement also are entitled to confidential treatment because their disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy," 5 U.S.C. § 552(b)(7)(C). As the Third Circuit has explained, the purpose of FOIA Exemption 7(C) is to "provid[e] broad protection to entities involved in law enforcement investigations in order to encourage cooperation with federal regulators," and "[c]orporations ... involved in law enforcement investigations ... face public embarrassment, harassment, and stigma because of that involvement." *AT&T Inc. v. FCC*, 582 F.3d 490, 498 n.5 (3<sup>rd</sup> Cir. 2009), *cert. granted*, *FCC v. AT&T Inc.*, No. 09-1279, 177 L. Ed. 2d 1151; 2010 U.S. LEXIS 5745; 79 U.S.L.W. 3193 (September 28, 2010).

Google has not made the information redacted in the Second Supplement available to the public, or to third parties other than to the Connecticut State Attorney General. Google believes it is necessary for the Commission to maintain the confidentiality of this information throughout the investigation and thereafter until it is destroyed.

Consistent with 47 C.F.R. § 0.459(d)(1), Google respectfully requests notification by the Commission if release of the redacted material in the Response is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
*Counsel to Google Inc.*

Enclosures

cc: Hillary DeNigro, Investigations and Hearings Division, Enforcement Bureau  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@ojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

December 20, 2010

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W., Room TW-A325  
Washington, DC 20554

Attn: Mindy Littell  
Investigations and Hearings Division  
Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

Re: **Google Inc., File No. EB-10-IH-4055**

Dear Ms. Dortch:

On behalf of Google Inc. ("Google"), we submit herewith a copy of Google's Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint ("Motion"), filed December 17, 2010 with the U.S. District Court, Northern District of California, in Case No. 5:10-md-02184 JW (HRL), and ask that the Motion be associated with Google's responses to the letter dated November 3, 2010 from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission, in the above-referenced matter.

Kindly contact me should there be any questions regarding this matter.

Respectfully submitted,



E. Ashton Johnston  
*Counsel for Google Inc.*

Enclosure

cc: Hillary DeNigro, Investigations and Hearings Division, Enforcement Bureau  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lujlaw.com

tel (202) 887-6230  
fax (202) 887-6231

December 20, 2010

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W., Room TW-A325  
Washington, DC 20554

Attn: Mindy Littell  
Investigations and Hearings Division  
Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

FILED/ACCEPTED

DEC 20 2010

Federal Communications Commission  
Office of the Secretary

Re: Google Inc., File No. EB-10-IH-4055

Dear Ms. Dortch:

On behalf of Google Inc. ("Google"), we submit herewith a copy of Google's Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint ("Motion"), filed December 17, 2010 with the U.S. District Court, Northern District of California, in Case No. 5:10-md-02184 JW (HRL), and ask that the Motion be associated with Google's responses to the letter dated November 3, 2010 from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission, in the above-referenced matter.

Kindly contact me should there be any questions regarding this matter.

Respectfully submitted,



E. Ashton Johnston  
Counsel for Google Inc.

Enclosure

cc: Hillary DeNigro, Investigations and Hearings Division, Enforcement Bureau  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau

1 DAVID H. KRAMER, State Bar No. 168452  
2 MICHAEL H. RUBIN, State Bar No. 214636  
3 BART E. VOLKMER, State Bar No. 223732  
4 CAROLINE E. WILSON, State Bar No. 241031  
5 WILSON SONSINI GOODRICH & ROSATI  
6 Professional Corporation  
7 650 Page Mill Road  
8 Palo Alto, CA 94304-1050  
9 Telephone: (650) 493-9300  
10 Facsimile: (650) 565-5100  
11 Email: mrubin@wsgr.com

12 *Attorneys for Defendant Google Inc.*

13 UNITED STATES DISTRICT COURT  
14 NORTHERN DISTRICT OF CALIFORNIA  
15 SAN JOSE DIVISION

16 IN RE GOOGLE INC. STREET VIEW  
17 ELECTRONIC COMMUNICATIONS  
18 LITIGATION

19 CASE NO.: 5:10-md-02184 JW (HRL)

20 **DEFENDANT GOOGLE INC.'S**  
21 **MOTION TO DISMISS**  
22 **PLAINTIFFS' CONSOLIDATED**  
23 **CLASS ACTION COMPLAINT**

24 Hearing Date: March 21, 2011  
25 Time: 9:00 a.m.  
26 Before: Honorable James Ware  
27  
28



## TABLE OF CONTENTS

	<u>Page</u>
NOTICE OF MOTION & MOTION DISMISS .....	1
STATEMENT OF ISSUE TO BE DECIDED .....	1
MEMORANDUM OF POINTS & AUTHORITIES .....	1
I. INTRODUCTION .....	1
II. FACTUAL BACKGROUND .....	2
A. Wi-Fi Technology. ....	2
B. Google's Geo-Location Services. ....	2
C. Google's Payload Collection.....	3
D. The Putative Class Action Lawsuits.....	3
III. ARGUMENT .....	5
A. Plaintiffs Have Failed To State A Federal Wiretap Act Claim. ....	5
1. Plaintiffs Have Failed To Plead Facts Showing That Their Wi-Fi Radio Broadcasts Were Not "Readily Accessible To The General Public." .....	6
2. Plaintiffs Cannot Plead Facts Supporting A Claim That Their Wi-Fi Radio Broadcasts Were Not "Readily Accessible To The General Public." .....	8
a. Plaintiffs Cannot Plead Facts Alleging That Their Wi-Fi Radio Broadcasts Were "Scrambled Or Encrypted." .....	8
b. Plaintiffs' Cannot Plead Facts Alleging That Their Wi-Fi Radio Broadcasts Meet Any Other Exception to the "Readily Accessible" Presumption.....	11
B. Plaintiffs' State Law Wiretap Claims Fail. ....	12
1. Plaintiffs' State Wiretap Claims Are Expressly Preempted .....	13
2. Plaintiffs' State Wiretap Claims Are Barred Based On Field Preemption. ....	14
3. Plaintiffs' State Wiretap Claims Are Barred Based On Conflict Preemption. ....	15
C. Plaintiffs' Section 17200 Claim Should Be Dismissed.....	16
1. Plaintiffs' Section 17200 Claim Is Preempted.....	17

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

2.	Plaintiffs Have Not Stated A Section 17200 Claim.....	17
3.	Plaintiffs Have Not Demonstrated Proposition 64 Standing.....	18
IV.	CONCLUSION .....	20

# TABLE OF AUTHORITIES

## Page

### CASES

1	<i>Ashcroft v. Iqbal</i> , 129 S. Ct. 1937 (2009) .....	5, 7
2	<i>Bank of Am. v. City &amp; Cnty. of S.F.</i> , 309 F.3d 551 (9th Cir. 2002) .....	13
3	<i>Bansal v. Russ</i> , 513 F. Supp. 2d 264 (E.D. Pa. 2007) .....	13
4	<i>Bardin v. Daimlerchrysler Corp.</i> , 136 Cal. App. 4th 1255 (2006) .....	17, 18
5	<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001) .....	15
6	<i>Bell v. Axiom Corp.</i> , No. 4:06CV00485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) .....	19
7	<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007) .....	7
8	<i>Berryman v. Merit Property Mgmt. Inc.</i> , 152 Cal. App. 4th 1544 (2007) .....	17
9	<i>Birdsong v. Apple, Inc.</i> , No. 06-2280, 2008 WL 7359917 (N.D. Cal. June 13, 2008) .....	7, 18
10	<i>Birdsong v. Apple, Inc.</i> , 590 F.3d 955 (9th Cir. 2009) .....	19
11	<i>Buckman Co. v. Plaintiffs' Legal Comm.</i> , 531 U.S. 341 (2001) .....	16
12	<i>Bunnell v. MPAA</i> , 567 F. Supp. 2d 1148 (C.D. Cal. 2007) .....	13, 14
13	<i>Butler v. Adoption Media, LLC</i> , 486 F. Supp. 2d 1022 (N.D. Cal. 2007) .....	19
14	<i>Connecticut Nat. Bank v. Germain</i> , 503 U.S. 249 (1992) .....	13
15	<i>Crowley v. CyberSource Corp.</i> , 166 F. Supp.2d 1263 (N.D. Cal. 2001) .....	8
16	<i>Facebook, Inc. v. Power Ventures, Inc.</i> , No. C 08-05780, 2010 WL 3291750 (N.D. Cal. July 20, 2010) .....	10, 18
17	<i>Freeman v. DirecTV, Inc.</i> , 457 F.3d 1001 (9th Cir. 2006) .....	8
18	<i>Fujitsu Ltd. v. Netgear Inc.</i> , 620 F.3d 1321 (Fed. Cir. 2010) .....	2, 11
19	<i>Howard v. America Online, Inc.</i> , 208 F.3d 741 (9th Cir. 2000) .....	12
20	<i>In re Nat'l Sec. Agency Telecomms. Records Litig.</i> , 483 F. Supp. 2d 934 (N.D. Cal. 2007) .....	14
21	<i>Kariguddaiah v. Wells Fargo Bank, N.A.</i> , No. C 09-5716, 2010 WL 2650492 (N.D. Cal. July 1, 2010) .....	17
22	<i>Key v. DSW, Inc.</i> , 454 F. Supp. 2d 684 (S.D. Ohio 2006) .....	19
23	<i>Kniesel v. ESPN</i> , 393 F.3d 1068 (9th Cir. 2005) .....	2

1	<i>Leadsinger, Inc. v. BMG Music Publ'g</i> , 512 F.3d 522 (9th Cir. 2008).....	8
2	<i>McKinney v. Google, Inc.</i> , No. 10-01177 JW, slip op. (N.D. Cal. Nov. 16, 2010).....	12
3	<i>Pub. Util. Dist. No. 1 of Grays Harbor Cnty. Washington v. IDACORP Inc.</i> , 379 F.3d 641 (9th Cir. 2004).....	14
4	<i>Quintero Family Trust v. OneWest Bank, F.S.B.</i> , No. 09-cv-1561, 2010 WL 392312 (S.D. Cal. Jan. 27, 2010).....	16
5	<i>Quon v. Arch Wireless</i> , 445 F. Supp. 2d 1116 (C.D. Cal. 2006), <i>rev'd on other</i> <i>grounds</i> , 529 F.3d 892 (9th Cir. 2008).....	13, 14, 15, 16
6	<i>Robinson v. HSBC Bank USA</i> , -- F. Supp. 2d --, 2010 WL 3155833 (N.D. Cal. Aug. 9, 2010).....	18
7	<i>Ruiz v. Gap, Inc.</i> , 540 F. Supp. 2d 1121 (N.D. Cal. 2008).....	18, 19
8	<i>Sanders v. Apple Inc.</i> , 672 F. Supp. 2d 978 (N.D. Cal. 2009) .....	18
9	<i>Schmier v. U.S. Court of Appeals</i> , 279 F.3d 817 (9th Cir. 2002).....	5
10	<i>Schulken v. Washington Mut. Bank</i> , No. 09-02708, 2009 WL 4173525 (N.D. Cal. Nov. 19, 2009).....	17
11	<i>Silvas v. E*Trade Mortg. Corp.</i> , 514 F.3d 1001 (9th Cir. 2008) .....	13, 15, 16
12	<i>Snow v. DirecTV, Inc.</i> , 450 F. 3d 1314 (11th Cir. 2006) .....	6, 7, 8
13	<i>Spiegler v. Home Depot U.S.A., Inc.</i> , 552 F. Supp. 2d 1036 (C.D. Cal. 2008).....	18
14	<i>Tellabs, Inc. v. Makor Issues &amp; Rights, Ltd.</i> , 551 U.S. 308 (2007) .....	5
15	<i>United States v. Ahrndt</i> , No. 08-468, 2010 WL 373994 (D. Ore. Jan. 28, 2010) .....	10
16	<i>United States v. Santos</i> , 553 U.S. 507 (2008) .....	9
17	<i>Walker v. Geico Gen. Ins. Co.</i> , 558 F.3d 1025 (9th Cir. 2009).....	18

## STATUTES

21	18 U.S.C. § 2510, <i>et seq.</i> .....	<i>passim</i>
22	18 Pa C.S.A. § 5703, <i>et seq.</i> .....	15
23	Cal. Bus. & Prof. Code § 17200.....	<i>passim</i>
24	Cal. Bus. & Prof. Code § 17204.....	18
25	M.S.A. § 626A.01, <i>et seq.</i> .....	15
26	MO St. § 542.200, <i>et seq.</i> .....	15
27	N.R.S. § 200.610, <i>et seq.</i> .....	15
28	R.C. § 2933.51, <i>et seq.</i> .....	15

1	SC St. § 17-30-10, <i>et seq.</i> .....	15
2	Tex. Civ. Prac. & Rem. § 123.001, <i>et seq.</i> .....	15

## RULES

3	47 C.F.R. § 15, <i>et seq.</i> .....	11
4	Fed. R. Civ. P. 12(b)(6) .....	1, 5, 8

## MISCELLANEOUS

Benjamin D. Kern, <i>Whacking, Joyriding And War-Driving: Roaming Use Of Wi-Fi And The Law</i> , 21 Santa Clara Computer & High Tech L.J. 101, 138 (2004) .....	9
S. Rep. No. 99-541 (1986), <i>reprinted in</i> 1986 U.S.C.C.A.N. 3555 .....	7, 9, 12, 15

1                                    **NOTICE OF MOTION & MOTION DISMISS**

2            Please take notice that on March 21, 2011, at 9:00 a.m., before the Honorable James  
3    Ware, Defendant Google Inc. ("Google") will and hereby does move to dismiss with prejudice  
4    plaintiffs' Consolidated Class Action Complaint ("CCAC"). Google's motion is based on this  
5    notice, the accompanying memorandum of points and authorities, the declaration of Michael H.  
6    Rubin, the pleadings on file in these actions, arguments of counsel and any other matters that the  
7    Court deems appropriate.

8                                    **STATEMENT OF ISSUE TO BE DECIDED**

9            Does the CCAC state a claim for which relief can be granted under Rule 12(b)(6)?

10                                  **MEMORANDUM OF POINTS & AUTHORITIES**

11    I.        **INTRODUCTION**

12            This case concerns Google's acquisition of radio broadcasts sent over open, unencrypted  
13    Wi-Fi networks. Google, like many other companies, collects and uses the presence of Wi-Fi  
14    networks to offer "location aware" services, like Google Maps. By allowing individuals to  
15    pinpoint their location using the identified Wi-Fi networks around them, Google can provide  
16    those people with directions and other location-specific information. Prior to mid-May 2010,  
17    Google collected the publicly available identifying information that Wi-Fi networks broadcast by  
18    using radio antennae mounted to cars that drove down public streets. If, at the instant Google  
19    drove by, a user was broadcasting data over an identified network and the network was  
20    configured to be open and unencrypted, Google also collected the data (known as "payload  
21    data") that was being broadcast.

22            Shortly after Google announced that it had collected this payload data, lawyers from  
23    across the country rushed to file more than a dozen putative class-action lawsuits alleging that  
24    Google violated the federal Wiretap Act and other laws. These lawsuits are misguided: it is not  
25    unlawful under the Wiretap Act to receive information from networks that are configured so that  
26    communications sent over them are "readily accessible to the general public." 18 U.S.C.  
27    § 2511(2)(g)(i). Because plaintiffs have already represented that their broadcasts took place over  
28    open, unencrypted networks, any broadcasts that Google acquired were, by the Wiretap Act's



1 plain language, "readily accessible to the general public." For that reason, Google did not violate  
2 the Wiretap Act by collecting payload data.<sup>1</sup>

3 Plaintiffs' parallel state wiretap claims fail for the identical reason, and because the  
4 federal Wiretap Act preempts those claims. Plaintiffs' claim under Section 17200 of the  
5 California Business and Professions Code is also preempted, and fails because plaintiffs have not  
6 sufficiently alleged the "actual injury" and "loss of money or property" that the statute requires.

7 In sum, the CCAC does not state a claim upon which relief can be granted and should be  
8 dismissed with prejudice.

## 9 II. FACTUAL BACKGROUND

### 10 A. Wi-Fi Technology.

11 Wi-Fi is a wireless communications protocol that uses radio waves to broadcast  
12 information pursuant to the IEEE 802.11 standard. *See* Rubin Dec., Ex. 4 at ¶ 9<sup>2</sup>; *see also*  
13 *Fujitsu Ltd. v. Netgear Inc.*, 620 F.3d 1321, 1325 (Fed. Cir. 2010). Wi-Fi is commonly used to  
14 connect computers and mobile devices to routers providing Internet access. *See* Rubin Dec., Ex.  
15 3 at 1; *Fujitsu*, 620 F.3d at 1325. Each Wi-Fi-compliant device is assigned by its manufacturer a  
16 unique number called a MAC address. *See* Rubin Dec., Exs. 1, 2, 3, 4 at ¶ 8. In addition,  
17 wireless access points like routers are assigned alpha-numeric names called service set identifiers  
18 ("SSIDs"). *Id.*, Exs. 1, 2, 3, 4 at ¶ 16. Most mobile phones and computers can detect a router's  
19 MAC Address and SSID. *Id.*

### 20 B. Google's Geo-Location Services.

21 Google has long used vehicles to drive down public streets in order to take photographs  
22 of their surroundings for use in its Street View service. For a time, those vehicles also collected

23  
24 <sup>1</sup> As it has stated repeatedly, Google does not want the payload data it collected, did not and  
25 will not use the payload data in any product or service, and has taken steps to ensure that payload  
26 data is not collected again. But Google's acknowledgement that the collection was an error does  
27 not render Google's conduct unlawful, nor excuse plaintiffs from the pleading requirements  
28 mandated by the unambiguous language of the Wiretap Act.

<sup>2</sup> Rubin Declaration Exhibits 1, 2, 3, and 4 are all incorporated by reference into the CCAC.  
*See, e.g.*, CCAC ¶¶ 66, 69-72, 80. Accordingly, this Court may consider them. *See Knievel v.*  
*ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

1 identifying information regarding available Wi-Fi networks. CCAC ¶¶ 2, 4. To accomplish this,  
2 the vehicles were outfitted with readily available open source software and radio antennae.  
3 Rubin Dec., Ex. 4 at ¶¶ 23-28. The process by which Google identified available networks is  
4 similar to what happens when a person turns on his laptop or mobile phone to find Wi-Fi  
5 networks at a hotel, a coffee shop, or anywhere else. Because the presence of any Wi-Fi network  
6 acts as a unique landmark, knowing which combination of networks is nearby at a given time  
7 allows Google to help people determine their approximate locations based on which networks  
8 they can detect. The collection of publicly broadcast Wi-Fi network identification information is  
9 a common practice, and plaintiffs take no issue with it.

10 **C. Google's Payload Collection.**

11 On April 27, 2010, Google published a blog post stating that its Street View cars had  
12 been collecting SSID and MAC address information about Wi-Fi networks, but not payload data.  
13 CCAC ¶ 69; Rubin Dec., Ex. 1. Shortly thereafter, Google determined that its Street View  
14 vehicles were also collecting payload data that was publicly broadcast over open, unencrypted  
15 networks at the moment Google's vehicles drove by. CCAC ¶ 71; Rubin Dec., Ex. 2. Google  
16 quickly corrected its prior post and described the scope of the payload collection. CCAC ¶ 71;  
17 Rubin Dec., Ex. 2.

18 On June 9, 2010, Google released a report from an independent security firm that had  
19 analyzed, among other things, how Google collected public Wi-Fi radio broadcasts. Rubin Dec.,  
20 Exs. 2, 4. The report describes how Google used freely available open-source software to  
21 passively collect radio broadcasts from Wi-Fi networks as its cars traveled down the road. By  
22 cycling through Wi-Fi channels five times per second, the software limited any single data-  
23 acquisition to two-tenths of one second. *Id.*, Ex. 4 at ¶ 28. The report confirmed that only  
24 payload data that was broadcast over open, unencrypted networks was collected. *Id.*, Ex. 4 at ¶  
25 20.

26 **D. The Putative Class Action Lawsuits.**

27 Since mid-May 2010, 19 putative class-action lawsuits have been filed across the country  
28 concerning Google's acquisition of payload data. The complaints collectively included the



1 following claims for relief: (1) the federal Wiretap Act; (2) the federal Computer Fraud and  
2 Abuse Act; (3) the federal Stored Communications Act; (4) Section 705 of the federal  
3 Communications Act; (5) state wiretap statutes; (6) common law privacy torts; (7) state data  
4 protection statutes; (8) conversion; (9) unjust enrichment; (10) trespass; (11) unfair competition;  
5 (12) accounting; and (13) California Penal Code Section 502. Most of plaintiffs' original  
6 complaints premised liability on Google's alleged acquisition of payload data broadcast over  
7 "open" or "open [and] unencrypted" networks. None of the plaintiffs named in the CCAC have  
8 alleged that they configured their Wi-Fi network to be closed or encrypted.<sup>3</sup> See Appendix A  
9 (chart detailing plaintiffs' prior statements that their networks were open and unencrypted,  
10 including (i) plaintiffs' core allegations in their original complaints, and (ii) the first joint case  
11 management statement in this action).

12 The parties filed motions with the Judicial Panel on Multidistrict Litigation ("MDL  
13 Panel") to have the extant cases transferred to a single court for pre-trial activities. On August  
14 17, 2010, the MDL panel concluded that transfer was appropriate because the cases were  
15 predicated on the shared factual allegation that Google had acquired information from "class  
16 members' *open, non-secured wireless networks*." See MDL August 17, 2010 Transfer Order at 1  
17 (emphasis added), Docket No. 1. Eight other cases were transferred by related case orders issued  
18 by this Court. Docket Nos. 17, 31, 48; Rubin Dec., Ex. 5. Two other cases were conditionally  
19 transferred by the MDL Panel. Docket Nos. 32, 59. All of these actions are consolidated for  
20 pre-trial purposes before this Court. See Docket No. 53.

21 On November 8, 2010, plaintiffs filed a consolidated complaint. The CCAC contains  
22 only three claims for relief: (1) the federal Wiretap Act; (2) state law wiretap statutes; and  
23 (3) California's Business and Professions Code Section 17200. Plaintiffs allege that Google's  
24 Street View vehicles used "packet sniffers" to collect "all types of data sent and received over  
25

26 <sup>3</sup> Notably, the group of plaintiffs in the *Berlage* case had amended their complaint to add a  
27 new plaintiff, Denise Bergin, who alleged that she used a "closed or encrypted wireless network  
28 and internet connection." Rubin Dec., Ex. 11 (*Berlage* First Am. Compl. at ¶¶ 8, 15). Of the  
*Berlage* plaintiffs, Ms. Bergin alone was chosen to be excluded from the case upon filing of the  
CCAC.

1 the Wi-Fi connections.” CCAC ¶ 4. Plaintiffs do not allege that Google used Wi-Fi payload  
2 data in any product or service. Instead, they plead that Google merely “stored the data on its  
3 servers.” *Id.* at ¶ 6.

### 4 III. ARGUMENT

5 Under Rule 12(b)(6), a complaint should be dismissed when it “fail[s] to state a claim  
6 upon which relief can be granted.” Fed. R. Civ. P. 12(b)(6). “[O]nly a complaint that states a  
7 plausible claim for relief survives a motion to dismiss.” *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1950  
8 (2009). While the Court accepts as true all material allegations in the complaint, it need not  
9 accept the truth of conclusory allegations or unwarranted inferences, nor should it accept legal  
10 conclusions as true merely because they are cast in the form of factual allegations. *Id.* at 1949.  
11 (“Threadbare recitals of the elements of a cause of action, supported by mere conclusory  
12 statements, do not suffice.”); *Schmier v. U.S. Court of Appeals*, 279 F.3d 817, 820 (9th Cir.  
13 2002). On a motion to dismiss, the Court may consider “documents incorporated into the  
14 complaint by reference, and matters of which a court may take judicial notice.” *Tellabs, Inc. v.*  
15 *Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

16 Here, the CCAC fails to state a claim upon which relief can be granted. Because  
17 plaintiffs cannot cure the CCAC’s pleading deficiencies through amendment, the CCAC should  
18 be dismissed with prejudice.

#### 19 A. Plaintiffs Have Failed To State A Federal Wiretap Act Claim.

20 The federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, prohibits the intentional interception  
21 of wire, oral, or electronic communications. 18 U.S.C. § 2511(1)(a). Plaintiffs’ Wiretap Act  
22 claim here is based on the allegation that Google acquired “electronic communications” sent  
23 over “WiFi networks.” CCAC ¶¶ 1, 18-38, 129. The radio waves broadcast by those Wi-Fi  
24 networks (“Wi-Fi Radio Broadcasts”) are the “electronic communications” at issue in this case.  
25 See 18 U.S.C. § 2510(10) (defining “electronic communication” to include those that occur “in  
26 whole or in part” by radio). But, as noted, plaintiffs have admitted that their Wi-Fi networks  
27 were configured to be “open,” or “open [and] unencrypted.” See Appendix A. That is fatal to  
28 their wiretapping allegations. It is not unlawful under the Wiretap Act to acquire information

1 from networks configured in a way that makes communications sent over them “readily  
2 accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i); *Snow v. DirecTV, Inc.*, 450 F.3d  
3 1314, 1320-21 (11th Cir. 2006) (“Congress did not intend to criminalize or create civil liability  
4 for acts of individuals who ‘intercept’ or ‘access’ communications that are otherwise readily  
5 accessible by the general public.”). Plaintiffs’ Wi-Fi Radio Broadcasts were “readily accessible  
6 to the general public” under the Wiretap Act. That is confirmed by the plain text of the statute,  
7 its structure, and the case law.

8 **1. Plaintiffs Have Failed To Plead Facts Showing That Their Wi-Fi**  
9 **Radio Broadcasts Were Not “Readily Accessible To The General**  
10 **Public.”**

11 To state a claim under the Wiretap Act, a plaintiff must plead facts showing that their  
12 communications were not “readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i)  
13 (“It shall not be unlawful ... to intercept or access an electronic communication made through an  
14 electronic communication system that is configured so that such electronic communication is  
15 readily accessible to the general public”); see *Snow*, 450 F.3d at 1321 (describing pleading  
16 requirements and stating: “the requirement that the electronic communication not be readily  
17 accessible by the general public is material and essential to recovery”).

18 All radio broadcasts, including plaintiffs’ Wi-Fi Radio Broadcasts, are by statutory  
19 definition “readily accessible to the general public” unless they are:

- 20 (A) scrambled or encrypted;
- 21 (B) transmitted using modulation techniques whose essential  
22 parameters have been withheld from the public with the intention  
23 of preserving the privacy of such communication;
- 24 (C) carried on a subcarrier or other signal subsidiary to a radio  
25 transmission;
- 26 (D) transmitted over a communication system provided by a common  
27 carrier, unless the communication is a tone only paging system  
28 communication; or
- (E) transmitted on frequencies allocated under part 25, subpart D, E, or  
F of part 74, or part 94 of the Rules of the Federal  
Communications Commission, unless, in the case of a  
communication transmitted on a frequency allocated under part 74

1 that is not exclusively allocated to broadcast auxiliary services, the  
communication is a two-way voice communication by radio.

2 18 U.S.C. § 2510(16)(A)-(E) (defining what "readily accessible to the general public" means  
3 with respect to radio communications). Thus, a radio broadcast is "readily accessible to the  
4 general public" unless the plaintiff has pled facts to support one of the five exceptions set forth  
5 above.

6 A clear policy animates the statute: anyone may freely receive radio broadcasts as a  
7 matter of course unless the broadcast is scrambled or encrypted, uses particular modulation  
8 techniques, or is transmitted using specified non-public systems or frequencies. S. Rep. No. 99-  
9 541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 ("Radio communications are considered  
10 readily accessible to the general public unless they fit into one of five specified categories.").  
11 These are objective technical standards; the subjective beliefs or expectations of the broadcaster  
12 concerning public accessibility are irrelevant. S. Rep. No. 99-541, at 18 (Section 2511(2)(g)(i)  
13 creates "an objective standard of design configuration for determining whether a system receives  
14 privacy protection").

15 Plaintiffs do not even attempt to plead facts showing that their Wi-Fi Radio Broadcasts  
16 fall within one of the five narrow exceptions to the "readily accessible" presumption for radio  
17 broadcasts. Without a single supporting fact, plaintiffs merely recite the bare legal conclusion  
18 that their Wi-Fi Radio Broadcasts were "not readily accessible to the general public." CCAC ¶¶  
19 18-38, 130, 142. That is insufficient. *See Ashcroft*, 129 S. Ct. at 1949 ("A pleading that offers  
20 'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action will not  
21 do.'") (citations omitted); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007); *Snow*, 450 F.3d  
22 at 1321 (conclusory allegation that website was not readily accessible insufficient); *Birdsong v.*  
23 *Apple, Inc.*, No. 06-2280, 2008 WL 7359917, at \*3 (N.D. Cal. June 13, 2008) ("Plaintiffs' legal  
24 conclusion . . . is insufficient. Rather, a plausible set of facts must either be alleged or be  
25 apparent to the Court upon which Plaintiffs could prevail."). These plaintiffs must plead facts,  
26 which, if taken as true, would bring their broadcasts within Section 2510(16). *Snow*, 450 F.3d at  
27 1321 ("To survive a motion to dismiss, [plaintiff] must have alleged, at a minimum, facts from  
28



1 which we could infer that his electronic bulletin board was not readily accessible to the general  
2 public.”). They have not done so and their Wiretap Act claim should be dismissed. *See, e.g.,*  
3 *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1009 (9th Cir. 2006) (affirming dismissal of ECPA  
4 case under Rule 12(b)(6) based on the plain language of the statute); *Crowley v. CyberSource*  
5 *Corp.*, 166 F. Supp. 2d 1263, 1265-72 (N.D. Cal. 2001) (dismissing under Rule 12(b)(6) a  
6 putative class action brought under the Wiretap Act and ECPA).

7                   **2. Plaintiffs Cannot Plead Facts Supporting A Claim That Their Wi-Fi**  
8                   **Radio Broadcasts Were Not “Readily Accessible To The General**  
9                   **Public.”**

10 Plaintiffs would not be able to cure the pleading defects in the CCAC by amendment  
11 because the exceptions to the “readily accessible” presumption are at odds with the facts  
12 plaintiffs have pled and the central premise of their case. Accordingly, no leave to amend should  
13 be granted. *See, e.g., Leadsinger, Inc. v. BMG Music Publ’g*, 512 F.3d 522, 532 (9th Cir. 2008)  
(leave to amend should not be granted when doing so would be futile).

14                   **a. Plaintiffs Cannot Plead Facts Alleging That Their Wi-Fi Radio**  
15                   **Broadcasts Were “Scrambled Or Encrypted.”**

16 Plaintiffs have not alleged in the CCAC that they configured their Wi-Fi networks to be  
17 “scrambled or encrypted.” 18 U.S.C. § 2510(16)(A). Nor could they given their repeated  
18 admissions that they broadcast using *open, unencrypted* wireless networks:

- 19           • Each plaintiff “used and maintained at all times relevant and  
20           material hereto an unencrypted wireless internet connection at his  
21           home.” Berlage First Am. Compl. ¶¶ 5-7 (Rubin Dec., Ex. 10).
- 22           • “During all relevant times [plaintiffs] used an open Wi-Fi network  
23           at their residence.” Carter Compl. ¶ 6 (Rubin Dec., Ex. 9).
- 24           • “During all times relevant herein, [plaintiff] used and maintained  
25           an open wireless internet connection at his home which he shares  
26           with his wife and family.” Colman Compl. ¶ 5 (Rubin Dec., Ex.  
27           7).
- 28           • Plaintiffs “maintained and used an open wireless internet  
            connection.” Van Valin Compl. ¶¶ 4-5 (Rubin Dec., Ex. 6).

*See also* Appendix A.

1        Instead of asserting that they scrambled or encrypted their networks, plaintiffs allege that  
2 it takes sophisticated technology to acquire their publicly available Wi-Fi Radio Broadcasts.  
3 See, e.g., CCAC ¶ 55. Regardless of whether that allegation is true, it is entirely beside the point.  
4 The Wiretap Act is clear that all radio broadcasts are open to the public unless the system over  
5 which they are sent scrambles or encrypts them. See 18 U.S.C. § 2511(2)(g)(i); 18 U.S.C.  
6 § 2510(16)(A). The legislative history confirms this plain meaning and instructs that anyone  
7 wishing to invoke the “scrambled or encrypted” exception for radio networks must configure  
8 their networks to convert their “signal[s] into unintelligible form.” S. Rep. No. 99-541, at 15.  
9 The encryption inquiry does not turn on the sophistication of radio receivers, but on the technical  
10 network configuration steps that one must take to render a radio broadcast unintelligible to the  
11 public. *Id.*<sup>4</sup> Plaintiffs here have not alleged that they configured their networks to encrypt or  
12 scramble their Wi-Fi Radio Broadcasts. They have alleged the opposite – that their networks  
13 were open and unencrypted – and that permanently dooms their wiretap claim. See Benjamin D.  
14 Kern, *Whacking, Joyriding And War-Driving: Roaming Use Of Wi-Fi And The Law*, 21 Santa  
15 Clara Computer & High Tech L.J. 101, 138 (2004) (the definition of “readily accessible” with  
16 respect to radio broadcasts “removes all Wi-Fi networks that do not use encryption from the  
17 ECPA’s protection.”).<sup>5</sup>

18  
19 <sup>4</sup> The Senate Report leaves no room for debate about what constitutes scrambling or  
20 encryption: “These terms are used in their technical sense. To ‘encrypt’ or to ‘scramble’ means  
21 to convert the *signal* into unintelligible form by means intended to protect the contents of a  
22 communication from unintended recipients. Methods which merely change the form of a  
23 plaintext message, e.g., a device which converts an analog signal to a digital stream, does not  
24 provide ‘encryption’ within the meaning of this bill.” S. Rep. No. 99-541 at 15 (emphasis  
25 added).

26  
27 <sup>5</sup> Plaintiffs include a smattering of allegations in the CACC about the alleged scarcity of  
28 devices that could acquire their Wi-Fi Radio Broadcasts. Such incorporeal allegations offer no  
future salvation. The notion that alleged scarcity of receiving devices is relevant to the encryption  
or scrambling analysis is foreclosed not only by the statute itself, but also by the rule of lenity.  
That canon of statutory interpretation “requires ambiguous criminal laws to be interpreted in favor  
of the defendants subjected to them.” *United States v. Santos*, 553 U.S. 507, 514, 523 (2008) (rule  
applies to statutes like the Wiretap Act that have both civil and criminal applications). And the  
rule would be violated by an interpretation of “scrambled or encrypted” that allowed liability to be  
found one day based on a supposed scarcity of receiving devices, but not the next when such  
devices passed some undefined threshold of prevalence. See *id.* at 514 (the rule of lenity ensures  
that “no citizen should be held accountable for a violation of a statute whose commands are

(continued...)

1        Given that plaintiffs did not scramble or encrypt their Wi-Fi Radio Broadcasts, there is no  
2        doubt that those broadcasts were “readily accessible to the general public” under §2510(16)(A) of  
3        the Wiretap Act. Indeed, in a similar case, the district court in Oregon recently held just that. *See*  
4        *United States v. Ahrndt*, No. 08-468, 2010 WL 373994 (D. Or. Jan. 28, 2010). In *Ahrndt*, a woman  
5        logged on to her neighbor’s open Wi-Fi network and accessed an iTunes folder on his personal  
6        computer that appeared to contain child pornography. *Id.* at \*1. She alerted the police, and an  
7        officer came to her house and duplicated her steps. *Id.* That led to search warrants and the  
8        defendant’s arrest. *Id.* at \*1-\*2. The defendant moved to suppress on the ground, *inter alia*, that  
9        the officer violated the Wiretap Act by using the defendant’s open Wi-Fi network to access the  
10       computer files at issue. The Court rejected that position because “defendant’s wireless network  
11       system was configured so that any electronic communications emanating from his computer via his  
12       iTunes program were readily accessible to any member of the general public with a Wi-Fi enabled  
13       laptop.” *Id.* at \*8.

14       The logic of *Ahrndt*—that files accessed directly on the defendant’s home computer were  
15       “readily accessible to any member of the general public” because his Wi-Fi network was  
16       configured to be open and unsecured—compels the conclusion that the Wi-Fi Radio Broadcasts in  
17       this case are likewise “readily accessible to the general public” under the statute. *See id.* at \*1,  
18       \*8. Indeed, the defendant’s files in *Ahrndt* were far less accessible to the general public than  
19       plaintiffs’ Wi-Fi Radio Broadcasts were here. The materials in that case resided on the  
20       defendant’s personal computer in his home and were not broadcast onto the street over radio  
21       waves. To access the materials at issue in *Ahrndt*, the police needed to take a number of  
22       volitional steps: (1) logging on to the defendant’s network; (2) accessing his iTunes library;  
23       (3) viewing the folder structure; (4) opening a folder; and (5) opening a file. In sharp contrast,  
24       plaintiffs base their Wiretap claim on Google’s passive, non-targeted collection of Wi-Fi Radio

25       (...continued from previous page)  
26       uncertain, or subjected to punishment that is not clearly prescribed.”); *Facebook, Inc. v. Power*  
27       *Ventures, Inc.*, No. C 08-05780, 2010 WL 3291750, at \*11 (N.D. Cal. July 20, 2010) (rejecting  
28       statutory interpretation under rule of lenity that would allow liability to be predicated on web sites’  
     malleable user agreement as that “would create a constitutionally untenable situation in which  
     criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use”).

1 Broadcasts transmitted publicly over open, unencrypted networks as Google Street View vehicles  
2 passed by.

3 \* \* \*

4 Given plaintiffs' prior admissions about their use of open, unencrypted Wi-Fi networks, it  
5 would be futile to provide them an opportunity to try to plead that the Wi-Fi Radio Broadcasts  
6 were not "readily accessible to the general public" because they were "scrambled or encrypted."  
7 18 U.S.C. § 2510(16)(A).

8 **b. Plaintiffs Cannot Plead Facts Alleging That Their Wi-Fi Radio**  
9 **Broadcasts Meet Any Other Exception To The "Readily**  
10 **Accessible" Presumption.**

11 It would be equally futile to allow plaintiffs to try to plead that their Wi-Fi Radio  
12 Broadcasts were not readily accessible based on one of the other provisions of 18 U.S.C. §  
13 2510(16)(B-E).

14 **First**, plaintiffs cannot plead that their Wi-Fi Radio Broadcasts were "transmitted using  
15 modulation techniques whose essential parameters have been withheld from the public with the  
16 intention of preserving the privacy of such communication." 18 U.S.C. § 2510(16)(B).  
17 Unencrypted Wi-Fi communications are transmitted pursuant to detailed parameters set forth in  
18 federal regulations and using a standard—802.11—that has been publicized widely and discussed  
19 in patents, industry groups, business literature, and the press. *See* 47 C.F.R. § 15 *et seq.*; *Fujitsu*,  
20 620 F.3d at 1325. The point of having a standard govern Wi-Fi broadcasts is so that businesses  
21 and individuals may know precisely how the protocol works to enable them to build and use  
22 interoperable devices and systems. *See, e.g., Fujitsu*, 620 F.3d at 1325 ("Products in this industry  
23 adhere to standards to ensure interoperability."). Because the standard is by design open to the  
24 public, plaintiffs cannot meet this exception.

25 **Second**, plaintiffs cannot allege that their Wi-Fi Radio Broadcasts were "carried on a  
26 subcarrier or other signal subsidiary to a radio transmission." 18 U.S.C. § 2510(16)(C).  
27 Subcarrier and subsidiary radio transmissions relate to collateral information that accompanies  
28 commercial radio and television broadcasts; they have nothing to do with Wi-Fi. *See* S. Rep. No.  
99-541, at 15 ("this category includes, for example, data and background music services carried



1 on FM subcarriers. It also includes data carried on the Vertical Blanking Interval (VBI) of a  
2 television signal.”).

3 **Third**, plaintiffs cannot allege that their Wi-Fi Radio Broadcasts were “transmitted over  
4 a communication system provided by a common carrier.” 18 U.S.C. § 2510(16)(D). Plaintiffs  
5 are natural persons who plainly do not qualify for common-carrier status. Nor would some new  
6 allegation that their Wi-Fi networks were “provided by” an Internet Service Provider (“ISP”)   
7 change the result. ISPs that offer enhanced services like Internet access are not regulated as  
8 common carriers. See *Howard v. America Online, Inc.*, 208 F.3d 741, 752 (9th Cir. 2000);  
9 *McKinney v. Google, Inc.*, No. 10-01177 JW, slip op. at 13-14 (N.D. Cal. Nov. 16, 2010)  
10 (“Internet Service Providers are generally not common carriers.”).

11 **Fourth**, plaintiffs could not claim that their Wi-Fi Radio Broadcasts were sent over the  
12 specific non public radio frequencies referenced in 18 U.S.C. § 2510(16)(E). Wi-Fi  
13 transmissions do not use those frequencies. And this subsection of the Wiretap Act shows that  
14 Congress knows how to place entire radio frequencies off-limits from consumption by the  
15 general public. If Congress had wanted to create a blanket prohibition on the acquisition of Wi-  
16 Fi transmissions, it had an easy and ready mechanism to do so. But it did not. Hence,  
17 unencrypted Wi-Fi radio broadcasts are readily accessible to the general public.

18 \* \* \*

19 The plain text and structure of the Wiretap Act make clear that the radio broadcasts at  
20 issue in this case were “readily accessible to the general public.” Under Section 2511(2)(g)(i),  
21 there can be no Wiretap Act liability.

22 **B. Plaintiffs’ State Law Wiretap Claims Fail.**

23 In addition to the federal Wiretap Act, plaintiffs have asserted claims under the wiretap  
24 laws of Arizona, Hawaii, Minnesota, Nebraska, Ohio, South Carolina, Utah, Tennessee, Missouri,  
25 Washington, Pennsylvania, Nevada and Texas. CCAC ¶ 141. Plaintiffs allege that these statutes  
26 are “substantially similar to 18 U.S.C. § 2511.” *Id.* These claims must be dismissed for the same  
27 reason that plaintiffs’ federal Wiretap Act claim fails: plaintiffs’ Wi-Fi Radio Broadcasts were  
28

1 "readily accessible to the general public." Regardless, the state wiretap claims should be  
2 dismissed based on federal preemption.

3 Federal law may preempt state law in three ways: (1) expressly; (2) by pervasive  
4 regulation demonstrating implicit intent to displace state law in a particular field; or (3) where  
5 there is a conflict between state law and federal law and enforcement of the state law "stands as  
6 an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."  
7 *Silvas v. E\*Trade Mortg. Corp.*, 514 F.3d 1001, 1004 (9th Cir. 2008) (quoting *Bank of Am. v.*  
8 *City & Cnty. of S.F.*, 309 F.3d 551, 558 (9th Cir. 2002)). All three doctrines of preemption bar  
9 plaintiffs' state wiretap claims here.

#### 10 L. Plaintiffs' State Wiretap Claims Are Expressly Preempted.

11 The Wiretap Act contains an express preemption clause: "[t]he remedies and sanctions  
12 described in this chapter with respect to the interception of electronic communications are the  
13 only judicial remedies and sanctions for nonconstitutional violations of this chapter involving  
14 such communications." 18 U.S.C. § 2518(10)(c) (emphasis added). Yet plaintiffs assert state  
15 wiretap law claims because they allegedly "provide a remedy *in addition* to the Federal Wiretap  
16 Statute." CCAC ¶ 144 (emphasis added). The federal statute is unambiguous, and any  
17 "additional remedies" that plaintiffs seek from state laws are preempted. See *Connecticut Nat.*  
18 *Bank v. Germain*, 503 U.S. 249, 253-54 (1992) ("We have stated time and again that courts must  
19 presume that a legislature says in a statute what it means and means in a statute what it says  
20 there."); *Bunnell v. MPAA*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (holding federal Wiretap  
21 Act expressly preempts parallel state law claims); *Quon v. Arch Wireless*, 445 F. Supp. 2d 1116,  
22 1138 (C.D. Cal. 2006) ("Only those remedies outlined in the [statute] are the ones, save for  
23 constitutional violations, that a party may seek for conduct prohibited by the [statute]."), *rev'd on*  
24 *other grounds*, 529 F.3d 892 (9th Cir. 2008).<sup>6</sup>

25  
26 <sup>6</sup> Some courts have ruled that the Wiretap Act's preemption clause operates only to prevent  
27 the exclusion of evidence in a criminal proceeding. See, e.g., *In re Nat'l Sec. Agency*  
28 *Telecomms. Records Litig.*, 483 F. Supp. 2d 934, 938-39 (N.D. Cal. 2007); *Bansal v. Rusy*, 513  
F. Supp. 2d 264, 282-83 (E.D. Pa. 2007). Those constructions should be rejected because they  
conflict with the plain language of the Wiretap Act, which precludes all other remedies. See 18  
U.S.C. § 2518(10)(c).

2. Plaintiffs' State Wiretap Claims Are Barred Based On Field Preemption.

In addition to being expressly preempted, plaintiffs' state wiretap claims also fail based on field preemption. That doctrine applies where federal law "is sufficiently comprehensive to infer that Congress left no room for supplementary regulation by the states. When the federal government completely occupies a given field or an identifiable portion of it . . . the test of preemption is whether the matter on which the state asserts the right to act is in any way regulated by the federal government." *Pub. Util. Dist. No. 1 of Grays Harbor Cnty. Washington v. IDACORP Inc.*, 379 F.3d 641, 647 (9th Cir. 2004) (internal quotation marks and citations omitted). This is the case here.

The federal Wiretap Act, as amended by ECPA in 1986, comprehensively regulates privacy claims concerning electronic communications. See 18 U.S.C. §§ 2510-22.<sup>7</sup> As a matter of law, this detailed regulatory scheme setting forth privacy standards for electronic communications leaves no room for supplementary state regulation. See *Bunnell*, 567 F. Supp. 2d at 1154-55 (dismissing plaintiff's state wiretap act claims because "[t]he scheme of the ECPA is very comprehensive: it regulates private parties' conduct, law enforcement conduct, outlines a scheme covering both types of conduct and also includes a private right of action for violation of the statute. As such, it is apparent to this Court that Congress left no room for supplementary state regulation.") (internal quotation marks and citations omitted); cf. *Quon*, 445 F. Supp. 2d at 1138 (holding that ECPA preempts state law invasion of privacy and constitutional law claims because "[t]he intricacies of the regulatory scheme crafted by the ECPA (and the SCA) are fairly

<sup>7</sup> Section 2511 proscribes the circumstances in which private parties and government officials may intercept, disclose or use electronic communications. 18 U.S.C. § 2511(1). The Act also sets forth in detail numerous instances where interception is lawful, notwithstanding the prohibitions contained in Section 2511(1). 18 U.S.C. § 2511(2). Violators of Section 2511 face criminal penalties, see 18 U.S.C. § 2511(4), and suit by the federal government for the interception of certain satellite and radio communications, see 18 U.S.C. § 2511(5). Sections 2512 and 2513 regulate the manufacture and possession of interception devices. See 18 U.S.C. §§ 2512-13. Sections 2515 through 2519 describe the manner in which electronic communications may be lawfully intercepted and used by government officials. See 18 U.S.C. §§ 2515-19. And Section 2520 provides a private right of action for any person whose electronic communication has been unlawfully intercepted. See 18 U.S.C. § 2520.

1 comprehensive: Regulating private parties' conduct, law enforcement efforts to uncover stored  
2 electronic communications, and devising a fairly complicated scheme to accomplish both,  
3 including a private right of action for violations of the statute's provisions.").

4 The original Wiretap Act was Congress's response, "in a comprehensive fashion," to an  
5 evolving need to provide for the security of communications while also authorizing certain  
6 interceptions. S. Rep. No. 99-541, at 2. When it enacted ECPA in 1986, Congress extended the  
7 Wiretap Act to include a pervasive legal regime governing electronic communications, including  
8 radio communications. *See Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001). Congress could not  
9 have intended to allow the states to disrupt that effort by enforcing their own disparate—and  
10 conflicting—set of laws and remedies regarding electronic-communications privacy.<sup>8</sup> And  
11 because the patchwork of state laws plaintiffs assert here do just that, the claims based on those  
12 laws should be dismissed with prejudice under the doctrine of field preemption.

13 **3. Plaintiffs' State Wiretap Claims Are Barred Based On Conflict**  
14 **Preemption.**

15 Plaintiffs' state wiretap claims are also barred based on conflict preemption. The federal  
16 government authorized the unlicensed radio spectrum for public use to encourage innovation in  
17 wireless communications technology without governmental interference. Plaintiffs' state wiretap  
18 claims would erect an "obstacle to the accomplishment and execution of the full purposes and  
19 objectives" of that policy. *Silvas*, 514 F.3d at 1004 (citation omitted). For many years, the FCC  
20 prohibited public use of unlicensed radio frequencies altogether. Rubin Dec., Ex. 16 (FCC  
21 Docket No. 81-413 at 1). But in 1985, the FCC opened up three bands of the spectrum for  
22 unlicensed use, including the 2.4 GHz band over which Wi-Fi network routers broadcast. *Id.* at 9.  
23 The Commission did so to encourage "rapid development" of civilian wireless technologies with  
24 minimal governmental interference. *Id.* at 11. The following year, Congress decided that all  
25

26 <sup>8</sup> Some of the state laws vary the available civil remedies. *See* M.S.A. § 626A.01, *et seq.*;  
27 Ohio R.C. § 2933.51, *et seq.*; SC St. § 17-30-10, *et seq.*; 18 Pa C.S.A. § 5703, *et seq.* And still  
28 others are antiquated and mirror the pre-ECPA federal Wiretap Act. *See* MO St. § 542.200, *et*  
*seq.*; N.R.S. § 200.610, *et seq.*; Tex. Civ. Prac. & Rem. § 123.001, *et seq.*





1 have failed to plead facts stating a substantive Section 17200 violation; and (3) plaintiffs have not  
2 alleged adequately the loss of "money or property" to demonstrate Proposition 64 standing.

3 **1. Plaintiffs' Section 17200 Claim Is Preempted.**

4 Just like the state wiretap claims, plaintiffs' Section 17200 claim is preempted by federal  
5 law because it concerns the alleged interception of radio communications. Federal law provides  
6 the exclusive avenue for such claims. *See, supra*, Section III.B.

7 **2. Plaintiffs Have Not Stated A Section 17200 Claim.**

8 In any event, plaintiffs have failed to plead facts to support a Section 17200 claim.  
9 Plaintiffs assert claims under the "unlawful" and "unfair" prongs of California's unfair  
10 competition law ("UCL"). CCAC ¶¶ 136-37. The "unlawful" prong necessarily fails because, for  
11 the reasons stated above, Google's collection of Wi-Fi Radio Broadcasts from open, unencrypted  
12 Wi-Fi networks was not unlawful. *See Kariguddaiah v. Wells Fargo Bank, N.A.*, No. C 09-5716,  
13 2010 WL 2650492, at \*7 (N.D. Cal. July 1, 2010) (dismissing § 17200 claim due to plaintiff's  
14 failure to state a claim for either breach of contract or wrongful foreclosure upon which the §  
15 17200 claim was based); *Berryman v. Merit Property Mgmt. Inc.*, 152 Cal. App. 4th 1544, 1554  
16 (2007) ("Thus, a violation of another law is a predicate for stating a cause of action under" the  
17 "unlawful" prong).

18 The basis for plaintiffs' invocation of the "unfair" prong is difficult to discern, and that is  
19 reason enough to dismiss their UCL claim. *See Schulken v. Washington Mut. Bank*, No. 09-  
20 02708, 2009 WL 4173525, at \*8 (N.D. Cal. Nov. 19, 2009) ("the Court finds that Plaintiffs' UCL  
21 claim fails because Plaintiffs have not alleged sufficient facts to give Defendants notice of what  
22 fraudulent or unfair conduct is being asserted against them"). Regardless, the CCAC does not  
23 remotely plead facts that would support a UCL claim under that theory.

24 The law is unsettled regarding how to evaluate the "unfair" prong. Some courts have held  
25 that a plaintiff must plead facts showing a violation of a public policy that is "tethered to specific  
26 constitutional, statutory, or regulatory provisions." *Bardin v. Daimlerchrysler Corp.*, 136 Cal.  
27 App. 4th 1255, 1260-61 (2006). Other courts have articulated a more amorphous test under  
28 which conduct that is "immoral, unethical, oppressive, unscrupulous or substantially injurious to

1 consumers" may support liability. *Id.* at 1260. It does not matter which test the court employs  
2 here because plaintiffs have not stated a claim under either one.

3 Google's conduct was lawful under the Wiretap Act. It therefore cannot be immoral,  
4 unethical, oppressive, unscrupulous or violative of public policy. *See, e.g., Facebook, Inc.*, 2010  
5 WL 3291750, at \*15; *Sanders v. Apple Inc.*, 672 F. Supp. 2d 978, 989 (N.D. Cal. 2009). That  
6 leaves a single issue: whether the CCAC alleges facts supporting a claim that Google's actions  
7 were "substantially injurious to consumers." It does not. Plaintiffs merely allege that Google  
8 collected and stored payload data sent from open, unencrypted Wi-Fi networks and for a time  
9 stored that data on its servers. They do not claim that Google used that information or disclosed it  
10 to anyone. The CCAC does not describe any injury to consumers, let alone a substantial one.  
11 *See, e.g., Spiegler v. Home Depot U.S.A., Inc.*, 552 F. Supp. 2d 1036, 1044-47 (C.D. Cal. 2008);  
12 *Birdsong*, 2008 WL 7359917, at \*6 (rejecting "conjectural or hypothetical" injury claims under  
13 Section 17200). Plaintiffs' Section 17200 claim should be dismissed for failing to plead facts that  
14 would support liability.

### 15 3. Plaintiffs Have Not Demonstrated Proposition 64 Standing.

16 Plaintiffs' UCL claim also fails based on their failure to demonstrate Proposition 64  
17 standing. Section 17200 "requires a plaintiff to establish that it has 'suffered injury in fact and  
18 has lost money or property.'" *Walker v. Gelco Gen. Ins. Co.*, 558 F.3d 1025, 1027 (9th Cir. 2009)  
19 (quoting Cal. Bus. & Prof. Code § 17204) (emphasis added); *Robinson v. HSBC Bank USA, – F.*  
20 *Supp. 2d –*, 2010 WL 3155833, at \*9 (N.D. Cal. Aug. 9, 2010) (dismissing with prejudice Section  
21 17200 claim where plaintiffs "have not and cannot allege lost 'money or property' and thus have  
22 no standing."). The CCAC does not allege facts meeting this requirement.

23 Plaintiffs do not assert that they lost money, but plead in conclusory fashion that they lost  
24 "property." CCAC ¶ 138. The only "property" referenced in the CCAC is the data that plaintiffs  
25 broadcast over open, unencrypted Wi-Fi networks. Plaintiffs voluntarily sent out that information  
26 over a radio network without any plausible expectation of it being returned. Those broadcasts  
27 have not been "lost" under any definition of the term. *See Ruiz v. Gap, Inc.*, 540 F. Supp. 2d  
28 1121, 1127 (N.D. Cal. 2008) (rejecting claim of "loss of property" under Section 17200 over

1 personal information contained on a stolen laptop and noting the lack of authority for the  
2 proposition that the “unauthorized release of personal information constitutes a loss of property”).  
3 Nor is plaintiffs’ claim of entitlement to statutory damages sufficient to confer Section 17200  
4 standing. *See Butler v. Adoption Media, LLC*, 486 F. Supp. 2d 1022, 1062 (N.D. Cal. 2007).  
5 Plaintiffs have not demonstrated the loss of “money” or “property,” and their Section 17200 claim  
6 therefore should be dismissed.

7 Finally, plaintiffs would not be able to demonstrate the loss of “money” or “property” in  
8 an amended pleading. Their basic contention is that Google acquired payload data from open,  
9 unencrypted Wi-Fi networks. There are no allegations of subsequent use or disclosure of the  
10 payload collected. Nor is there any allegation from any plaintiff of actual injury resulting from  
11 Google’s conduct. On these facts, it would be impossible for plaintiffs to assert that they  
12 somehow lost “money” or “property” because their Wi-Fi transmissions were collected and sat on  
13 Google’s servers. *See Bell v. Axiom Corp.*, No. 4:06CV00485, 2006 WL 2850042 (E.D. Ark.  
14 Oct. 3, 2006) (dismissing privacy class action where plaintiff failed to allege any tangible injury  
15 resulting from access to database containing consumer information); *Key v. DSW, Inc.*, 454 F.  
16 Supp. 2d 684 (S.D. Ohio 2006) (same). Accordingly, their Section 17200 claim should be  
17 dismissed with prejudice. *See, e.g., Birdsong v. Apple, Inc.*, 590 F.3d 955, 961-62 (9th Cir. 2009).



1           **IV.    CONCLUSION**

2           For the foregoing reasons, Google respectfully requests that the Court dismiss the CCAC  
3 with prejudice and enter judgment in Google's favor.

4  
5           Dated: December 17, 2010

Attorneys for Defendant Google Inc.

6  
7           By: /s/ Michael Rubin

8           David H. Kramer

9           Michael H. Rubin

10          Bart E. Volkmer

11          Caroline E. Wilson

12          Wilson Sonsini Goodrich & Rosati

13          650 Page Mill Road

14          Palo Alto, CA 94304-1050

15          Telephone: (650) 493-9300

16          Facsimile: (650) 565-5100

17          Email: mrubin@wsgr.com

## APPENDIX A

Appendix A: Plaintiffs' Prior Statements Regarding Their Use of Open, Unencrypted Wi-Fi Networks

Robin Dec. Ex. No.	Court Filing in which statement was made	Plaintiff Name	Statement
6	<i>Van Valin Complaint</i> (filed 5/17/10)  D. Or. Case No: 3:10-cv-00557-MO	Van Valin, Vicki	¶4: "During the class period, Van Valin used and maintained and used [sic] an open wireless internet connection ("WiFi connection") at her home."
7	<i>Colman Complaint</i> (filed 5/26/10)  D.D.C. Case No.: 1:10-cv-00877-JDB	Colman, Jeffrey	¶5: "During all times relevant herein, Colman used and maintained an open wireless internet connection at his home . . ."
8	<i>Keyes Complaint</i> (filed 5/28/10)  D.D.C. Case No.: 1:10-cv-00896-JDB	Keyes, Patrick	¶1: "Defendant intentionally intercepted electronic communications sent or received on open wireless connection ("WiFi connections") by the Class . . ."
9	<i>Carter Complaint</i> (filed 6/2/10)  E.D. Pa. Case No.: 2:10-cv-02649-JHS	Carter, Stephanie & Russell	¶6: "Plaintiffs Stephanie and Russell Carter, husband and wife, are residents of Philadelphia, PA. During all relevant times they used an open Wi-Fi network at their residence."  ¶7: "Plaintiffs used their open, unencrypted internet connection to transmit and receive personal and private data."
10	<i>Berlage First Amended Complaint</i> (filed 6/3/10)  N.D. Cal. Case No.: 5:10-cv-02187-JW (PVTx)	General Allegations	¶15: "[P]laintiffs Berlage, Linsky, and Fairbanks maintained open wireless network and internet connections at their residences, while plaintiff Bergin maintained a closed or encrypted wireless network and internet connection." <sup>1</sup>
		Berlage, Matthew	¶5: "Mr. Berlage used and maintained at all times relevant and material hereto an unencrypted wireless internet connection at his home . . . As used herein, 'unencrypted' is intended to mean that a 'key' was not needed to decode intercepted communications . . ."
		Linsky, Aaron	¶6: "Mr. Linsky used and maintained at all times relevant and material hereto an unencrypted wireless internet connection at his home . . . As used herein, 'unencrypted' is intended to mean that a 'key' was not needed to decode intercepted communications . . ."
		Fairbanks, James	¶7: "Mr. Fairbanks used and maintained at all times relevant and material hereto an unencrypted wireless internet connection at his home . . . As used herein, 'unencrypted' is intended to mean that a 'key' was not needed to decode intercepted communications . . ."

<sup>1</sup> Plaintiff Denise Bergin was excluded from the Consolidated Class Action Complaint ("CCAC").

**Appendix A: Plaintiffs' Prior Statements Regarding Their Use of Open, Unencrypted Wi-Fi Networks**

Rubin Dec. Ex. No.	Court Filing in which statement was made	Plaintiff Name	Statement
11	Loesin Complaint (filed 7/26/10)  N.D. Cal. Case No: 5:10-cv-03272-PVT	General Allegations	¶31: "At all relevant times, Plaintiffs have used open Wi-Fi network at their place of residence which are the type of networks susceptible to unauthorized access by Google Street View vehicles."
		Loesin, Jennifer	¶10: "Plaintiff Jennifer Loesin is a resident of Contra Costa County, California. During all relevant times, she used an open Wi-Fi network at her residence . . ."
		Blackwell, James	¶11: "Plaintiff James Blackwell is a resident of Alameda County, California. During all relevant times, he used an open Wi-Fi network at his residence . . ."
12	Jaffe Complaint (filed 9/9/10)  N.D. Cal. Case No.: 5:10-cv-04007-JW	Joffe, Benjamin	¶3: "During all times relevant herein, Plaintiff used and maintained an open, unencrypted wireless internet connection at his home."
13	Marigza Complaint (filed 9/10/10)  N.D. Cal. Case No.: 5:10-cv-04084-JW	General Allegations	¶21: "Plaintiffs Lilla Marigza, Wesley Hartline, David Binkley, and Blake Carter (collectively 'Class and Subclass Representative Plaintiffs') each consistently maintained an open wireless network at their homes since and through the time Google began collecting individuals' payload data with its GSV vehicles."
		Marigza, Lilla	¶3: "Plaintiff Lilla Marigza is an individual residing in Davidson County, Tennessee. During the class period, Mrs. Marigza used and maintained an open wireless connection ('WiFi connection') at her home."
		Hartline, Wesley	¶4: "Plaintiff Wesley Hartline is an individual residing in Davidson County, Tennessee. During the class period, Mr. Hartline used and maintained an open wireless connection ('WiFi connection') at his home."
		Binkley, David	¶5: "Plaintiff David Binkley is an individual residing in Davidson County, Tennessee. During the class period, Mr. Binkley used and maintained an open wireless connection ('WiFi connection') at his home."
14	Davis Complaint (filed 9/10/10)  N.D. Cal. Case No.: 5:10-cv-04079-JW	General Allegations	¶31: "At all relevant times, Plaintiffs have used an open Wi-Fi network at their place of residence . . ."
		Davis, Bertha	¶10: "Plaintiff BERTHA DAVIS is a resident of Solano County, California. During all relevant times, she used an open Wi-Fi network at her residence . . ."
		Taylor, Jason	¶11: "Plaintiff JASON TAYLOR is a resident of Alameda County, California. During all relevant times, he used an open Wi-Fi network at his residence . . ."

Appendix A: Plaintiffs' Prior Statements Regarding Their Use of Open, Unencrypted Wi-Fi Networks

Rubin Dec. Ex. No.	Court Filing in which statement was made	Plaintiff Name	Statement
15	<i>Myhre First Amended Complaint</i> (filed 9/17/10)  W.D. Wa. Case No. 2:10-cv-01444-JPD	Myhre, Eric	¶19: ""Plaintiff Eric Myhre is a United States citizen and resident of Seattle, Washington. Plaintiff used and maintained an unencrypted wireless internet connection at his home . . . .""
Dkt. No. 18 (not included in Rubin Dec.)	<i>Joint Case Management Statement</i> (filed 9/3/10)  N.D. Cal. Case No. 10-md-02184 -JW	Plaintiffs	¶2: "As the JPML stated in its Transfer Order, the principal factual issues 'aris[e] out of allegations that Google intentionally intercepted electronic communications sent or received over class members' open, non-secured wireless networks.'""



Google Inc.  
Public Policy Department  
1101 New York Avenue, NW  
Second Floor  
Washington, DC 20005



Phone 202.346.1100  
Fax 202.346.1101  
www.google.com

April 14, 2011

**CONFIDENTIAL TREATMENT REQUESTED**

***Via Hand Delivery and Email***

Mindy Littell  
Investigations and Hearings Division  
Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

Re: **Google Inc., File No. EB-10-IH-4055**

Dear Ms. Littell:

Google Inc. ("Google") hereby responds to the letter dated March 30, 2011 from Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission ("Bureau"), which requests supplemental information about Google's collection of payload data from Wi-Fi networks in the United States (the "Supplemental LOI"). As counsel for Google discussed with the Bureau, the one-week period provided to respond to the Supplemental LOI was not sufficient, and the Bureau agreed to extend the deadline so that Google may respond to the Supplemental LOI on April 14, 2011 and April 28, 2011.

In its December 10, 2010, responses to the Bureau's November 3, 2010 letter of inquiry (the "LOI"), Google provided a comprehensive statement of the events and circumstances surrounding the collection of Wi-Fi payload data in the United States. As noted there, Google's data collection in the United States involved the passive reception of publicly broadcast Wi-Fi information. Google has not disclosed the data to any third party; has not used the data in any product or service; and has not used the data for the benefit of any person or entity in any way. While Google acknowledged that the collection of Wi-Fi payload data did not meet its standards, nonetheless, Google did not violate Section 705 of the Communications Act or any other law. Comprehensive reviews previously undertaken by other agencies, including the Federal Trade Commission (which closed its investigation without action on October 27, 2010), have reached the same conclusion. We will continue to cooperate with the Bureau to work toward a prompt conclusion of this matter.

We ask that Google's responses to the Supplemental LOI be accorded confidential treatment, pursuant to the enclosed Request for Confidential Treatment.

Sincerely,

A handwritten signature in black ink, appearing to read "R. S. Whitt", written in a cursive style.

Richard S. Whitt

Enclosures

cc: Mindy Littel (by email) [Mindy.Littell@fcc.gov](mailto:Mindy.Littell@fcc.gov)  
Theresa Z. Cavanaugh (by email) [Terry.Cavanaugh@fcc.gov](mailto:Terry.Cavanaugh@fcc.gov)





**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-13**

From:

Sent: 5/15/2008 4:57 PM.

To: [ - ]

Cc: [ - ]

Bcc: [ - ]

Subject: Re: further [ - ] questions

[REDACTED]

We store the whole body of all non-encrypted data frames. One of my to-do items is to measure how many HTTP requests we're seeing.

>

>

> Thanks,





**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-14**

From: [REDACTED] Sent: 5/19/2008 5:31 PM  
To: [REDACTED]  
[ - ]  
Cc: [ - ]  
Bcc: [ - ]  
Subject:

[REDACTED] You might recall asking me about URLs seen over Wi-Fi from the cityblock cars... I got round to running a quick mapreduce. Out of 300M wi-fi packets, there were 70K HTTP requests for 32K unique URLs. Not many really.

me: Anyway, interesting statistics. I'd be curious to see a distribution. This kind of data could help our 'friends' at [REDACTED] :-)

me: Are you saying that these are URLs that you sniffed out of Wifi packets that we recorded while driving? 32k unique? How do you define unique? are two gmail.com URLs the same, for example?

me: Interesting anyway... Thanks for sharing.

[REDACTED] Plus the data was collected during daytime when most traffic is at work (and likely encrypted)

[REDACTED] I don't think the numbers are high enough for a good sample

[REDACTED] Top URL score was [REDACTED] with 250 hits from Tempe, AZ

[REDACTED] I measured uniqueness 2 ways: by URL directly, and by host name. 10K host names, gmail was top (1500) probably due to page refreshes.





**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

DOCUMENT 11-7

They will indeed be wardriving, but we have not yet given them the equipment to do it.

On 8/23/06, [REDACTED] wrote:

- > You've probably already investigated this, but we have all these
- > people driving around for the storefront mapping project -- is there
- > any possibility we can also have them wardriving at the same time?
- >



**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-9**

**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

DOCUMENT 11-7

Sent: 8/23/2006 8:41 PM.

They will indeed be wardriving, but we have not yet given them the equipment to do it.

On 8/23/06, [REDACTED] wrote:

- > You've probably already investigated this, but we have all these
- > people driving around for the storefront mapping project -- is there
- > any possibility we can also have them wardriving at the same time?
- >



**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-9**



From:

Sent: 10/31/2006 7:25 PM.

To: [ - ]

Cc: [ - ]

Bcc: [ - ]

Subject: Fw: Announcing GStumbler.

FYI

-----Original Message-----

From:

To:

Sent: Tue Oct 31 17:17:47 2006

Subject: Announcing GStumbler

Greetings!

I'd like to announce GStumbler, which will provide Wi-Fi scanning for Cityblock.

Design doc:

To build it:

please let me know what we need to do next to get this running on the vehicle.



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

April 14, 2011

*By Hand Delivery*

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of Google's responses to the March 30, 2011, letter to Google from Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission (the "Supplement LOI") in the above-referenced matter.

As shown below, some or all of Google's responses to each of the numbered requests in the Supplemental LOI contain information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential,"<sup>1</sup> and Exemption 7(C), which provides a statutory basis for withholding from public inspection information compiled for law enforcement purposes and that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."<sup>2</sup> We enclose herewith both a complete, unredacted copy of Google's responses, to be treated as confidential, and a separate copy of Google's responses marking specific portions thereof as Redacted.

Response to Supplemental Request No. 1. The redacted portions of Google's response to Supplemental Request No. 1 contain detailed, specific information regarding Google's private

---

<sup>1</sup> 5 U.S.C. § 552(b)(4). See also 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

<sup>2</sup> 5 U.S.C. § 552(b)(7)(C). See also 47 C.F.R. 0.457(g)(3).

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment

April 14, 2011

Page 2

business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company's internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). The Response also includes highly confidential and competitively sensitive information concerning the processes by which Google creates and produces its products. Google does not routinely disclose such information to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Supplemental Request No. 3. The redacted portion of Google's response to Supplement Request No. 3 contains detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Supplemental Request No. 4. The redacted portions of Google's response to Supplemental Request No. 4 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Supplemental Request No. 5. The redacted portions of Google's response to Supplemental Request No. 5 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Supplemental Request No. 6. The redacted portions of Google's response to Supplemental Request No. 5 contain detailed, specific information regarding Google's private



**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment

April 14, 2011

Page 3

business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Supplemental Request No. 7. The redacted portions of Google's response to Supplemental Request No. 7 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Supplemental Request No. 8. The redacted portion of Google's response to Supplemental Request No. 8 contains detailed, specific information regarding Google's private business and internal operations, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has not publicly disclosed the employees' identities, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google employees "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Response to Supplemental Request No. 9. The redacted portion of Google's response to Supplemental Request No. 9 contains detailed, specific information regarding Google's private business and internal operations, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has not publicly disclosed the employees' identities, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment  
April 14, 2011  
Page 4

Google employees "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989) contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Response to Supplemental Request No. 11. The redacted portion of Google's response to Supplemental Request No. 11 contains detailed, specific information regarding Google's private business and internal operations, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has not publicly disclosed the employees' identities, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google employees "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Response to Supplemental Request No. 12. The redacted portions of Google's response to Supplemental Request No. 12 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Supplemental Request No. 13. The redacted portions of Google's response to Supplemental Request No. 13 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment

April 14, 2011

Page 5

Response to Supplemental Request No. 14. The redacted portions of Google's response to Supplemental Request No. 14 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Documents. Unredacted Documents 11-1, 11-2, and 11-3, and Documents 11-7 through 11-15 are confidential and proprietary documents that contain detailed, specific information regarding Google's private business and internal operational actions and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). These Documents also contain trade secrets, including product design and computer code, which is highly confidential and competitively sensitive information. Google has not made any of these documents available to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and/or state attorneys general. Google believes it is necessary for the Commission to maintain the confidentiality of this information throughout the investigation and thereafter until it is destroyed.

Consistent with 47 C.F.R. § 0.459(d)(1), Google respectfully requests notification by the Commission if release of the redacted material in the Supplemental Responses is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
*Counsel to Google Inc.*

Enclosures

cc: Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau (by email)  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau (by email)





**RESPONSES OF GOOGLE INC. TO  
SUPPLEMENTAL LETTER OF INQUIRY  
FILE NO. EB-10-IH-4055**

**I. PRELIMINARY INFORMATION**

Google responds to the March 30, 2011 Letter of Inquiry (the “Supplemental LOI”) from Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission (“Bureau”).

**Request for Confidential Treatment.**

Enclosed herewith is Google’s Request for Confidential Treatment of Google’s responses covered by Exemptions 4 and 7(C) of the Freedom of Information Act (“FOIA”), which provides a statutory basis for withholding from public inspection “matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential” and “records or information ... that ... could reasonably be expected to constitute an unwarranted invasion of personal privacy.” 5 U.S.C. §§ 552(b)(4) & (7)(C). *See also* 47 C.F.R. § 0.457(d) (records not routinely available for public inspection include “trade secrets and commercial or financial information obtained from any person and privileged or confidential” under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

In addition, Google responds to the Supplemental LOI with the expectation and understanding that, consistent with Bureau practices and applicable law, details of the Bureau’s investigation will not be made public by any Commission employee.

**General Objections.**

Google objects to each question below that assumes or calls for a legal conclusion as to whether communications were “intercepted.” To the extent any of the following Requests include a reference to the term “intercept” or “interception,” Google’s response is without regard to the legal meaning of the term, does not constitute an admission that any communications were intercepted as a matter of law, and this objection applies.

Google objects to the Bureau’s use of the term “Wi-Fi data collection program at issue” in numerous questions below as undefined and ambiguous. Google understands the current inquiry to concern the collection of payload data through Street View cars.

Google objects to the supplemental request as unduly burdensome and overbroad.

Google objects to each question below to the extent it calls for the production of documents or information protected by the attorney-client privilege or the work product doctrine.

Google’s responses below are limited to the collection of payload data within the United States unless otherwise specifically identified.

## II. SPECIFIC RESPONSES TO REQUESTS FOR DOCUMENTS AND INFORMATION

The following responses are made subject to and without waiving Google's general objections.

**Supplemental Request No. 1:** Explain in detail the Company's privacy issue review process for new products or programs. In particular, describe any privacy issue review that occurred with respect to the program described in your response to LOI request no. 4, including when such review took place and the identity of all employees who participated in that review.

**Response to Supplemental Request No. 1:** [REDACTED]

Google produced the design document, marked confidential and proprietary, in response to LOI Request No. 11. Further, the design document called for the engineer to send it to a Google Product Counsel for review. The engineer failed to do so. Had he followed the review process, it would have been an opportunity at the outset for Google to identify the collection of payload data and prevent it. Accordingly, no privacy review for the collection of payload data took place until Google learned of the collection and halted it.











**Supplemental Request No. 2:** Explain in detail any Company engineering or other relevant protocol(s) for developing, reviewing and approving data collection programs and/or associated software, and provide documentation of those protocols.

**Response to Supplemental Request No. 2:** Google's Response to Supplemental Request No.1 includes the requested explanation.

**Supplemental Request No. 3:** Explain whether any peer review was conducted of the Wi-Fi data collection program at issue.

**Response to Supplemental Request No. 3:** As noted in its prior response to LOI Request No. 4, the engineer's design document and the code the engineer eventually wrote were made available to others to review if they so desired. No "peer review," as Google understands the term to mean either internal or third party scientific or engineering evaluation, was necessary for this project, beyond the confirmation that the code was bug-free and met style standards prior to checking it into Google's code repository.

**Supplemental Request No. 4:** State whether any patent applications have been filed and/or patents issued associated with the software used for the Wi-Fi data collection program at issue. If so, state the nature and/or classification of the application(s) filed, and when the applications were filed and/or the patents issued.

**Response to Supplemental Request No. 4:** No patent applications have been filed for the collection of Wi-Fi payload data.

**Supplemental Request No. 5:** Identify the length of the planning and development process for the Wi-Fi data collection program at issue, from conception to implementation. Provide the specific beginning and ending dates.

**Response to Supplemental Request No. 5:** The engineer began developing a means to collect Wi-Fi information using Street View vehicles in late 2006. He completed his design document on October 26, 2006 and the first executable version of the code was completed on October 31, 2006. The first test version of Wi-Fi collection hardware and software was deployed on Street View cars in November 2006. The production version of the Wi-Fi collection hardware and software was first launched in May 2007 and continued until early May 2010 when Google discovered the payload collection and ceased any Wi-Fi collection via Street View cars.

**Supplemental Request No. 6:** In response to LOI request no. 4, Google stated that Wi-Fi network data is used to improve the coverage and accuracy of the longitude and latitude coordinates assigned to the MAC addresses contained in Google's geolocation server, which in turn is used in the provision of location-based services.

a. Did the collection of payload data, in addition to the Wi-Fi network information, provide any additional improvement in such coverage or accuracy? Did it allow the Company to



enhance its location-based service offerings in any way? Was any other service, product, or database impacted in any way by the collection of payload data?

**Response to Supplemental Request No. 6.a:** No.

b. In response to LOI request no. 4, the Company stated that the Engineer who wrote the code to collect payload information believed that the collection of payload data “could be useful for search quality analysis.” Explain what is meant by “search quality analysis,” and in what way the Engineer believed that the collection of payload data could be useful for this purpose. Specifically explain how the collection of payload information, as distinct from the substance of the information, may be useful.

**Response to Supplemental Request No. 6.b:** The engineer believed that by mechanically extracting URLs from payload packets - an automated process that did not involve or require human review of the overall payload contents - he could obtain data showing Google Search usage that could be helpful in understanding the amount of people using Google’s search capability. This belief was theoretical, and as noted in response to LOI Request No. 5.b, the engineer purportedly informally asked a member of Google’s search quality team whether the data would be useful and was told it had no use or value. Having determined that there was no useful purpose for it, he abandoned the idea.

c. What other reasons, if any, did the Engineer provide for his proposal to collect “web traffic” information?

**Response to Supplemental Request No. 6.c:** None. Although it has no importance to the answer here or elsewhere in this supplemental response, the actual terminology used by the engineer in the design document was “traffic patterns” and “user traffic.” (See Document 11-1) Google’s use of the term “web traffic” was not intended to be a direct quote from the document.

**Supplemental Request No. 7:** With respect to the Company’s response to LOI request no. 4 concerning the purpose of the data collection and intended use of the communications, did the Company consider less privacy-invasive methods of accomplishing the Company’s stated objective (e.g., the development of Google’s geolocation server) that would not have involved the capture of “payload data.” If so, explain in detail what that alternative method was and why the Company did not employ it.

**Response to Supplemental Request No. 7:** As noted in LOI Response No. 4.a, the Wi-Fi network data, as opposed to the payload data, that Google collected in the United States was used in the development of Google’s geolocation server. As the Commission knows, Wi-Fi network information is publicly broadcast and used by many companies for location-related services or to identify available wireless Internet access points. Skyhook, for example, has licensed this information for many years to companies offering such services. The collection of payload data did not contribute to the goal of improving location-based services.

In regard to the payload itself, as noted in response to LOI Request No. 4, the engineer himself thought that the collection would not have a significant privacy impact because the Wi-Fi network data would not personally identify anyone or the precise physical location or address of the detected Wi-Fi access point. Further, as Google advised the Bureau in its prior response, and as confirmed in the report prepared by an independent technical services firm, Stroz Friedberg LLC (provided as Document 11-4 in response to the LOI), the software was designed to recognize encrypted networks and never to store payload data from those networks. Finally, the engineer believed that due to the constant motion and speed of the cars doing the collection, and because the software hopped Wi-Fi channels every two seconds, the information collected likely would be fragmented.

While Google has acknowledged that collection of the payload data broadcast from open and unencrypted wireless networks as its Street View cars drove by was not in keeping with its own standards, we note that passive receipt of such information by commercially available receivers was not inconsistent with industry standards. Off-the-shelf hardware and software was (and remains) commercially available to anyone to identify and receive Wi-Fi broadcasts that include both network information and payload. The Commission type-accepts and certifies wireless devices to operate in the approved Wi-Fi spectrum bands, and such devices are provided with default settings that configure Wi-Fi radio transmission to be open, unencrypted, and readily accessible to the general public if the user does not change the default settings.

**Supplemental Request No. 8:** In response to LOI request no. 4, the Company stated that “[t]he design document and the code the Engineer eventually wrote were made available to others to review if they so desired, but the significance of the Engineer’s reference to “web traffic” was not appreciated.” Identify all personnel who reviewed the referenced design document and code.

**Response to Supplemental Request No. 8:** The code was reviewed by [REDACTED] for proper syntax and de-bugging per Google’s process before checking it into Google’s code repository, and [REDACTED] worked with the code author to resolve a minor bug (unrelated to any payload collection) that was causing the program to shutdown. A configuration file related to the code was updated to reflect new hardware and that change was noted by [REDACTED] an engineer responsible for integrating the hardware on the Street View vehicles.

The gstumbler design document (Document 11-1) was made available by the engineer who wrote it [REDACTED] to his manager, [REDACTED] the tech lead for the Street View project; [REDACTED] a group of Street View team members; and the technical team for an unrelated Wi-Fi project (providing Wi-Fi access in Mountain View, CA). Google has not identified anyone who recalls having read the design document. The primary content of the design document in any event relates to the type of radio equipment to be used and its implementation on vehicles, not to the actual collection of data.

**Supplemental Request No. 9:** Request no. 4.h in the LOI instructed Google to identify “the business unit and individuals responsible for authorizing the interception or reception of such communications.” Google’s answer that “no member of senior management and no product group asked for payload to be collected” is not responsive. We again direct Google to identify

the business unit and individuals who authorized the interception or reception of payload communications, for instance, by authorizing the Engineer to install the relevant code in Street View equipment. In addition, explain in detail the process by which the use of this code was authorized – for instance, identify all documents that were prepared by the Engineer or others describing the code or requesting authorization to use it, identify all individuals who reviewed those documents, identify any individuals who authorized inclusion of the code in the software used in the Street View program, and state who authorized any expenditures in connection with installing and using the code. Provide copies of any documents that were prepared or reviewed in this process, or that refer to the Engineer's proposal and the approval of that proposal. Identify any individual who was involved in approving funding for the project.

**Response to Supplemental Request No. 9:** The engineer who wrote the code [REDACTED]

[REDACTED] he was asked by his supervisor [REDACTED] whether he could develop code to be used on Street View cars to collect Wi-Fi data for location-based services. [REDACTED] The engineer developed the code as part of Google's "20% program," which allows engineers to dedicate up to 20% of their time to work on projects of interest to them. The engineer developed, tested and made available the code for ultimate installation on the vehicles. (We previously provided the code and design documents to the Bureau in redacted form, and with this response, provide the unredacted versions subject to the Company's request for confidential treatment.) As we have explained, no one directed the engineer to collect the payload. When the Company discovered the collection, it terminated the activity promptly and disclosed the issue, confirming that the data had not been used in any product or service.

No equipment was necessary for the collection of Wi-Fi payload data beyond that used to collect freely available Wi-Fi network data. Apart from the reference in the design document to user traffic, [REDACTED]

[REDACTED] and a few subsequent communications that referenced the payload collection (see Documents 11-1, 11-3, and 11-7 to 11-15), there are no other responsive documents. There were no expenditures "in connection with installing or using the code." There were no approvals for funding for the project *per se* as the only costs involved were *de minimis* expenses related to commercially available radio receivers that were part and parcel of the cost of outfitting the Street View cars.

**Supplemental Request No. 10:** Provide a copy of any document that makes reference to the collection of "web traffic" in conjunction with the Engineer's proposal described in response to LOI request no. 4.

**Response to Supplemental Request No. 10:** Google has provided, subject to a request for confidential treatment, the only document (Document 11-1) that makes a reference to "traffic patterns" and "user traffic," which is the actual terminology used by the engineer.

**Supplemental Request No. 11:** Describe any testing of the software described in response to LOI request no. 4, either before or after installation in the Street View cars, to verify that it was

functioning as planned. Identify the individuals who did the testing or received the results, and provide any documents that reference such testing.

**Response to Supplemental Request No. 11:** At the outset of the program, the software was reviewed for proper syntax and de-bugging before it was checked into Google's code repository. After being installed in Street View cars in November 2006 for pre-launch testing of the Street View program in the United States, the software was tested for interoperability with attached hardware and other software installed in the vehicle. [REDACTED]

[REDACTED] It is important to understand that the compatibility testing with the vehicles was in regard to operational and technical matters, not the collection of payload or Wi-Fi network information. The Street View team's interest in compatibility was in regard to ensuring that the amount of data collected and stored on disks in the vehicles did not interfere with the storage of Street View images. The Wi-Fi data was a miniscule portion of the data collected by the cars and so had no impact.

**Supplemental Request No. 12:** State the cost of developing and implementing the program described in your response to LOI request no. 4.

**Response to Supplemental Request No. 12:** The actual cost of developing and implementing the program is not known. All hardware acquired for collecting Wi-Fi using Street View vehicles was off-the-shelf. [REDACTED]

[REDACTED] The Kismet software was open source and therefore without cost. The gstumbler code was developed in-house as previously explained. The storage of data in the Street View cars was incidental to storage capability already present in the vehicles.

**Supplemental Request No. 13:** Provide copies of any discovery responses (depositions, interrogatory responses, document responses or admissions) that the Company has provided to the plaintiff[s] in any private or class-action litigation concerning the collection of payload data by Street View cars in the United States.

**Response to Supplemental Request No. 13:** There have been no discovery requests in the pending civil actions in the United States.

**Supplemental Request No. 14:** Provide any information in the Company's possession about the actual or estimated number of individuals from whom the Company intercepted or received identifiable personal, financial, or password-related information as a result of the Wi-Fi data collection program. Include in your response information about impacted individuals both in the United States and abroad.

**Response to Supplemental Request No. 14:** As noted in response to LOI Request No. 2, Google does not know the actual or estimated number of individuals from whom payload data was collected, or the content of the payload data, and it has not analyzed the payload data to determine how many communications were received. As we previously explained, Google cannot even reliably identify the number of Wi-Fi devices from which communications were collected. Google can identify the number of basic service set identifiers (also known as



“BSSIDs”) which generally identify a single Wi-Fi access point that may be used by multiple stations, such as a laptop or other Wi-Fi-enabled device. The BSSID is the MAC address of the wireless access point, not the other devices, and does not indicate how many devices or networks connect through the access point itself. [REDACTED]

To be clear, this number indicates nothing about the number of users, networks, or devices from which communications may have been collected from any given access point. Nor does it indicate that payload data was collected from each access point. The BSSID is continuously broadcast whereas payload data would only have been collected if a user were sending or receiving information on an unencrypted network at the moment a Street View vehicle drove by. Finally, neither the BSSID nor any other Wi-Fi network information identified a specific person or address.

### **III. FURTHER SUPPLEMENT TO DECEMBER 10, 2010 RESPONSES TO LOI**

**Documents.** LOI Request No. 11 asked Google to provide copies of all Documents that provide the basis for or otherwise support Google’s responses to LOI Request Nos. 1-10. In its LOI Responses, and consistent with its discussions with the Bureau prior to submitting its LOI Responses, Google informed the Bureau that it had not undertaken a comprehensive review of email or other communications of potential record custodians. The Supplemental LOI directs Google to respond as instructed in the original LOI. Google has identified the documents responsive to the LOI and produces them herewith as Documents 11-7 through 11-15.

**Redacted Documents.** In its LOI Responses, Google provided redacted versions of Documents 11-1, 11-2, and 11-3. The Supplemental LOI directs Google to provide unredacted versions of these documents to the extent it did not do so in its December 14, 2010 and December 20, 2010 supplemental filings. Enclosed herewith are unredacted versions of the documents. The remaining redaction in Document 11-1 and 11-2 is a transmittal from in-house counsel to outside counsel on the first page of each document.



Google Inc.  
Public Policy Department  
1101 New York Avenue, NW  
Second Floor  
Washington, DC 20005



Phone 202.346.1100  
Fax 202.346.1101  
www.google.com

April 28, 2011

**CONFIDENTIAL TREATMENT REQUESTED**

***Via Hand Delivery and Email***

Mindy Littell  
Investigations and Hearings Division  
Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

Re: **Google Inc., File No. EB-10-IH-4055**

Dear Ms. Littell:

Google Inc. ("Google") hereby responds further to the letter dated March 30, 2011 from Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission ("Bureau"), which requests supplemental information about Google's collection of payload data from Wi-Fi networks in the United States (the "Supplemental LOI").

We ask that Google's responses to the Supplemental LOI be accorded confidential treatment, pursuant to the enclosed Request for Confidential Treatment.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard S. Whitt".

Richard S. Whitt

Enclosures

cc: Mindy Littell (by email) [Mindy.Littell@fcc.gov](mailto:Mindy.Littell@fcc.gov)  
Theresa Z. Cavanaugh (by email) [Terry.Cavanaugh@fcc.gov](mailto:Terry.Cavanaugh@fcc.gov)





# DECLARATION

I, [REDACTED] hereby declare under penalty of perjury of the laws of the United States that:

1. I am [REDACTED] at Google Inc. ("Google"),
2. I have reviewed and am familiar with the April 14, 2011 responses of Google ("Responses") to the March 30, 2011 letter to Google from Theresa Cavanaugh, Acting Chief, Investigations and Hearings Division of the Federal Communications Commission Enforcement Bureau. The Responses are true and correct to the best of my knowledge, information, and belief.

Dated: 4/25/2011





**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

April 28, 2011

*By Hand Delivery*

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of Google's further response to the March 30, 2011, letter to Google from Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission (the "Supplemental LOI") in the above-referenced matter.

Google's further response contains information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential,"<sup>1</sup> and Exemption 7(C), which provides a statutory basis for withholding from public inspection information compiled for law enforcement purposes and that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."<sup>2</sup> In particular, the further response contains information about privileged communications concerning the highly sensitive subject of the Street View Wi-Fi data collection, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google has not made this information available to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and/or state attorneys general. Google believes it is

---

<sup>1</sup> 5 U.S.C. § 552(b)(4). See also 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

<sup>2</sup> 5 U.S.C. § 552(b)(7)(C). See also 47 C.F.R. 0.457(g)(3).

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment

April 28, 2011

Page 2

necessary for the Commission to maintain the confidentiality of this information throughout the investigation and thereafter until it is destroyed.

We enclose herewith both a complete, unredacted copy of Google's further response, to be treated as confidential, and a separate copy marked as Redacted.

Consistent with 47 C.F.R. § 0.459(d)(1), Google respectfully requests notification by the Commission if release of the enclosed redacted material is requested pursuant to FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
*Counsel to Google Inc.*

Enclosures

cc: Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau (by email)  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau (by email)



1 wsgir  
1 R

1 wsgir

æyæy

ɹ|

ɹ| ɹ<sup>u</sup>ɹ|

ˈ d o c x

ˈ d o t x

ˈ t x z

ˈ t





## ATTACHMENT 4

**Office of the  
Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tel.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

**Commissariat  
à la protection de  
la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca



Files: 6100-010134  
6100-010141  
6100-010142

Mr. David T.S. Fraser  
McInnes Cooper  
Purdy's Wharf Tower II  
1300 – 1969 Upper Water Street  
PO Box 730  
Halifax, NS B3J 2V1

MAY 20 2011

Please find attached the report of findings prepared by this Office with regard to the complaints initiated by the Office of the Privacy Commissioner of Canada against Google Inc. under the *Personal Information Protection and Electronic Documents Act* (the Act), on May 31<sup>st</sup>, 2010.

Following the investigation into the complaints, we have concluded that, once fully implemented, Google's proposed remedial measures will meet the privacy issues underscoring our recommendations. As evidence of our Office's continuing intention to pursue this matter, we will be following up with Google next year to gauge full implementation of our recommendations. For details on the investigation and the rationale for our conclusion, please see the attached report of findings.

If you have any questions or comments about this letter, we would invite you to contact Jolana Klobouk, Privacy Investigator, at 1-800-282-1376.

Sincerely,

Chantal Bernier  
Assistant Privacy Commissioner

Attachment



## Executive Summary

### *Commissioner Initiated Complaint*

The investigation into Google Inc. (Google or the "respondent") by the Office of the Privacy Commissioner of Canada (OPC) comprised three allegations concerning the collection of personal information from unencrypted Canadian WiFi networks. The allegations were as follows:

- i. That Google collected personal information not limited to that which was necessary for purposes identified by the organization;
- ii. That Google collected the personal information of individuals without first identifying and disclosing the purposes for which that personal information was to be collected; and
- iii. That Google collected the personal information of individuals without their knowledge and consent.

### *Issues*

The central issue concerning the investigation was the unlawful collection of personal information. In May 2010, Google discovered that it had collected payload data from unsecured wireless networks in several countries, including Canada, during data gathering operations for its location-based services. "Payload" data constitutes the core information carried within a transmission unit (or "packet") over the internet. It can, depending on the nature of the communication, contain personal information. As such, our Office focused its investigation on the extent to which payload data collected by Google included the personal information of Canadians.

We also examined to what extent the purposes for which Google was collecting personal information from WiFi networks had been identified and disclosed prior to collection, and whether the individuals whose personal information had been collected had provided



meaningful consent. Although security issues were not specifically raised in the complaint, ensuring appropriate safeguards over the personal information collected figured prominently into our investigation.

### ***Findings and Conclusions***

On all three allegations – limiting collection, identifying purpose, and consent – our Office found Google to be in contravention of the *Personal Information Protection and Electronic Documents Act*, and concluded that the Commissioner-initiated complaints were well-founded. Google has agreed to fully adopt our Office's recommendations, and has already committed to the implementation of privacy controls and measures necessary to avoid a recurrence of this incident. Where well-founded allegations were deemed to be resolved, we have notified Google of our intention to seek independent verification of corrective measures implemented within one year from the date of this report.

## **REPORT OF FINDINGS**

### **Complaints under the *Personal Information Protection and Electronic Documents Act* (the Act)**

1. On May 31, 2010, the Office of the Privacy Commissioner of Canada initiated three complaints against Google Inc., pursuant to subsection 11(2) of the Act, having reasonable grounds to believe that the company had collected personal information from payload data originating from unencrypted Canadian WiFi networks.
2. The three complaints were as follows:
  - i. Google collected personal information not limited to that which was necessary for purposes identified by the organization (6100-010142);



- ii. Google collected the personal information of individuals without first identifying and disclosing the purposes for which that personal information was to be collected (6100-010141); and
  - iii. Google collected the personal information of individuals without their knowledge and consent (6100-010134).
3. Google was notified of the complaints on June 1, 2010. Initial representations were received from the company on June 29, 2010.
4. On July 19, 2010, our Office conducted a site-visit of Google's Mountain View facilities with regard to: (a) conducting a review of the payload data gathered by Google from Canadian WiFi networks; (b) inquiring into the circumstances surrounding the data collection incident; (c) ensuring the segregation and safe storage of Canadian payload data; and (d) discussing privacy risk mitigation measures under implementation. Supplementary meetings between our Office and Google's counsel were held by telephone and video-conference in August and September 2010.
5. Our Office issued a preliminary report of findings to Google on October 15, 2010. In our preliminary report we highlighted numerous concerns and recommendations. On February 1, 2011, following meetings with company representatives and counsel, Google submitted written representations in response to our recommendations. The present report of findings is the culmination of our investigation and consultations with Google.

## **Introduction**

6. In May 2010, following an audit request from the Hamburg Data Protection Authority in Germany, Google discovered that it had been collecting payload data from unsecured wireless networks as part of its collection of WiFi data. The collection is said to have occurred through data gathering operations for Google's location-based services (using the company's Street View cars).



7. Google contends that the collection of payload data was inadvertent. While the company intended to collect publicly broadcast SSID information and MAC addresses (i.e., information from WiFi networks and the unique numbers given to WiFi routers, respectively), it did not intend to collect payload data (i.e., the content of communications transmitted over these networks). In actual fact however, for the past several years, Google had been collecting samples of payload data from open (i.e., non-password-protected and unencrypted) WiFi networks throughout Canada and other countries.
8. According to Google, in early 2006 a company engineer working on an experimental WiFi project developed code capable of sampling categories of publicly broadcast WiFi data. In 2007, upon the launch of Google's mobile drive and the collection of basic WiFi network data for Google's geolocation services, that code was included in the software with which the company's Street View cars were equipped. It remains Google's contention that neither senior management nor the team leaders for the company's Street View project had sought or intended to actively use payload data.
9. To the company's credit, upon learning of its collection of personal information, Google grounded its Street View cars, stopped the collection of WiFi network data (effective May 7, 2010), segregated and stored all data collected, and notified government and law-enforcement officials of the incident (all with a view to deleting the data as soon as possible to minimize further privacy impacts).
10. Notwithstanding the above, Google is by its own admission a company which "pursue[s] ideas and products that often push the limits of existing technology"<sup>1</sup>. As such, and as a leader in information search, application and organization, it owes perhaps a special responsibility to those whose personal information it uses to ensure that its corporate innovations are balanced with appropriate levels of privacy protection.
11. Our role as a privacy regulator is critical. The purpose of the Act is to balance an organization's need to collect, use and disclose personal information for appropriate purposes with the individual's right to privacy vis-à-vis their personal information. Our role as a privacy educator and advocate is equally important however. Google's

<sup>1</sup> See Google Inc., *Privacy Principles*, available on-line at [http://www.google.com/intl/en/corporate/privacy\\_principles.html](http://www.google.com/intl/en/corporate/privacy_principles.html).



collection of private communications from cars travelling along city streets serves to highlight just how vulnerable open or unprotected WiFi communications can sometimes be, and just how accessible an individual's personal information may be when it travels along such paths.

12. While individuals are responsible for ensuring that they are fully informed of the risks associated with the adoption of new technologies, and for making use of appropriate and available privacy controls, organizations are responsible for ensuring that the privacy impacts of new programs and services have been fully considered prior to their introduction to the public. To be sure, cases such as the one before us help to shape the divide between personal and corporate responsibility and to develop new rules of engagement between the two parties. This report, like others before it, reflects our contribution to the development of those rules.

## **Limiting Collection**

### ***Allegation***

13. Based on information gathered prior to our investigation, our Office had reasonable grounds to believe that Google collected personal information not limited to that which was necessary for purposes identified by the organization, in contravention of Principle 4.4.1.<sup>2</sup>

### ***Summary of Investigation***

14. In order to ascertain the nature and extent of personal information collected by Google, our Office sent technical experts to Google's Mountain View location to sample and examine data sets collected by the company during its WiFi capture. The examination focussed on the identification of personal information within payload data captured during the period March 30, 2009 through May 7, 2010, during which Google's Street View cars were actively tracing Canadian roadways.

---

<sup>2</sup> Principles referred to in this report appear in Schedule 1 of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 [the Act].





15. By most estimates, Google is said to have collected approximately 600 gigabytes of data during its two year operation using Street View cars – in information terms, the rough equivalent to six floors of a university library. But not all of this data should be considered personal information.
16. Generally speaking, information becomes personal when it can be used to identify an individual. As Google's Street View cars were generally in motion during the collection of WiFi data, and where the company's in-car WiFi equipment regularly and automatically changed channels during data collection, the company was only able to collect fragments of payload data. In some cases, these data fragments could not be attached to an identifiable individual. In such cases, the information would not constitute "personal information" under the Act, even though the information in question may not have been benign.
17. In other cases, we found that the company had in fact collected personal information. Our sampling revealed, among other information, the full names, telephone numbers, and addresses of many Canadians. We also found complete email messages, along with email headers, IP addresses, machine hostnames, and the contents of cookies, instant messages and chat sessions.
18. Although our tests were designed to minimize further privacy intrusions, we were troubled to have found instances of particularly sensitive information, including computer login credentials (i.e., usernames and passwords), the details of legal infractions, and certain medical listings. While the raw data collected by Google would not always allow for perfect identification, the information collected was sufficiently capable of being linked to individuals through data matching or aggregation.

#### ***Application and Finding***

19. In making our determination on this issue, we applied Principle 4.4.1, and subsection 5(3) of the Act.
20. Principle 4.4.1 precludes organizations from collecting personal information indiscriminately. By law, the collection of personal information must be limited to that





which is necessary for the stated purposes of a project, as identified by an organization. Subsection 5(3) goes further to state that an organization may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

21. By the very nature of its operations – i.e., a secret and sweeping collection of data from open WiFi networks across Canada – Google violated the requirement that personal information be collected in a limited manner, and only for the stated purposes of the organization. Notwithstanding the fact the personal information collected was sourced from unprotected networks (and was in some cases fragmented), it is impossible to conceive that a reasonable person would have considered such collection appropriate in the circumstances.
22. Whereas our investigation revealed the indiscriminate collection of personal information – a fact not disputed by the company – we find Google to be in contravention of the above-cited principles, most notably Principle 4.4.1.

## **Identifying Purposes**

### ***Allegation***

23. Based on information gathered prior to our investigation, our Office had reasonable grounds to believe that Google collected the personal information of individuals without first identifying and disclosing the purposes for which that personal information was to be collected, in contravention of Principles 4.2, 4.2.1, and 4.2.2.

### ***Summary of Investigation***

24. According to its own stated Privacy Principles, Google strives to make the collection of personal information transparent.<sup>3</sup> Striving to be open about the information they have about individual users, and disclosing how that information is used to deliver its services is indeed a laudable goal. In many respects, it mirrors Principle 4.8 which requires that an organization make readily available to individuals specific

<sup>3</sup> *Supra* note 1 at paragraph 3.



information about its policies and practices relating to the management of personal information.

25. Unfortunately, notwithstanding the company's openness in disclosing the incident to the public and government authorities, in this case Google failed to live up to its own standards of transparency. During our investigation, we sought to uncover just how the failing occurred.
26. Regrettably the mistaken collection appears to have been entirely preventable. Given the nature of Google's business – "organizing the world's information"<sup>4</sup> – and the massive resources and expertise at its disposal, we would have expected Google to have had in place a more comprehensive privacy program, not to mention appropriate measures of control to ensure compliance with Canadian privacy laws.
27. In fact, Google does provide some level of privacy control and oversight over operations, in particular with respect to new projects involving the collection, use and storage of personal information. These processes however failed to operate as intended in the case at hand.
28. At the time of our investigation, Google had in place a formal review process for all external product launches. "External" products comprise all projects destined for public consumption or service. The review process, among other things, requires that an independent Product Counsel assess the privacy implications of all new programs. Not only is the review process mandatory, it is a first step in Google's elaborate code design procedures. According to Google, Product Counsel personnel consist of practicing lawyers, most of whom have some experience in privacy and information management.
29. As already reported by Google, the code that enabled the collection of payload data was first developed by the company in 2006 with a view to sampling certain categories of publicly broadcast WiFi data. At that time, the coding engineer believed that such information could prove useful to Google in the development of its future location-based services.

---

<sup>4</sup> Google's stated mission is to organize the world's information and make it universally accessible and useful.



30. In addition to recognizing the code's operational promise, Google's engineer, through the company's own code design procedures, identified several privacy concerns – in particular the fact that, with the code in question, Google would be capable of collecting sufficient data so as to precisely triangulate an individual's position. Unfortunately, these concerns were qualified by the engineer as merely "superficial privacy implications" and as such were not forwarded to Product Counsel Review, contrary to corporate convention.
31. Whereas the code in question was not properly reviewed for privacy impacts at the time of its development, it is perhaps surprising to note that it avoided any and all further privacy review even as it was being included in other Google programs. Despite the fact that a Product Counsel review is required in all instances where "internal" products are to be used or integrated in "external" offerings, the code in question was never reviewed for privacy impacts at the time it was to become operational. While the code had been reviewed for technical bugs and integration issues, it was never reviewed with the goal of identifying or examining the types of information that might be collected through its inclusion in Street View cars.
32. In explaining why the collection of payload data had not been discovered prior to 2010, Google explained that no one (except perhaps the originating engineer) believed that payload data could be useful in the company's foray into geolocational technologies. As such and where the engineer in question failed to fully comprehend the privacy implications of his or her work, a privacy review was never triggered. Google also contends that the payload data collected comprised such a minuscule amount of the total data being collected, that it had not raised sufficient concern to warrant a second look.
33. We believe that the issue is more than one of simple oversight however. The lack of concern for privacy issues emanating from the engineer's code, and the cursory privacy reviews conducted by managers during the code's acceptance and integration suggest, in our view, a far greater problem at Google. Notwithstanding the promise of its founding Privacy Principles, the incident in question suggests that Google employees may be suffering from a lack of privacy training and awareness. The company may also be lacking appropriate management structures to ensure privacy accountability.



---

### ***Application and Finding***

34. In making our determination on this issue, we applied Principles 4.2, 4.2.1, and 4.2.2.
35. Principle 4.2 requires that organizations identify the purposes for which personal information is to be collected at or before the time the information is collected. Principle 4.2.1 mandates that such purposes be properly documented and disclosed.
36. If Google never intended to collect payload data – or to use that data in any of its products – it follows that it was not in a position to properly identify the purposes for the collection of that information, or to seek the consent of individuals. Contrary to Principle 4.2.2 however, the company was in a position to examine and review the types of information it needed to collect and to cross-reference those needs with the type of information it was likely to collect in light of the code developed. Had it done so, it would likely have collected only that information which was required for the purposes that had been identified.
37. Whereas the company failed to appropriately determine and document the purposes for which personal information was needed prior to its collection, we find Google to be in contravention of the above-cited principles, most notably Principle 4.2.2.

## **Consent and Safeguards**

### ***Allegation***

38. Based on information gathered prior to our investigation, our Office had reasonable grounds to believe that Google collected the personal information of individuals without their knowledge and consent, in contravention of Principle 4.3.
-



---

### ***Summary of Investigation***

39. According to Google, the personal information of Canadians contained in payload data from open WiFi networks was collected unknowingly. It follows, that the consent of those individuals whose personal information was collected was not sought at the time of its collection.
40. To the company's credit, upon learning of its unauthorized collection of personal information, Google grounded its Street View cars, stopped the collection of WiFi network data, segregated and stored all data collected, and notified government and law-enforcement officials of the incident. Data saved to hard drives physically located in the company's fleet of Street View cars was subsequently transferred to Google's servers.
41. On May 15, 2010, Google consolidated Canadian payload data onto an encrypted hard drive. A second copy of the encrypted hard drive was made for security purposes during transportation, but has since been destroyed. Over the course of our investigation, Google provided sufficient assurances that the original media upon which Canadian data was collected had also been destroyed.
42. The encrypted drive containing Canadian payload data is presently held in a secure company location.

### ***Application and Finding***

43. In making our determination on this issue, we applied Principle 4.3. Principle 4.3 states that an individual's knowledge and consent are required for the collection, use, or disclosure of their personal information, except where inappropriate.
  44. We also considered Principle 4.5, which requires that personal information be retained for only as long as necessary for the fulfillment of stated purposes.
  45. We also considered Principle 4.7, which mandates that personal information be protected by security safeguards appropriate to the sensitivity of the information under an organization's control.
-



46. Finally, we considered Principle 4.1, which states that an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. In particular, we considered Principle 4.1.4, which requires organizations to implement policies and practices to give effect to the principles, including implementing procedures to protect personal information.
47. Whereas Google collected the personal information of individuals without their knowledge and consent prior to its collection, we find Google to be in contravention of Principle 4.3.
48. On the matter of information security, our investigation did not reveal evidence which would suggest that Google had failed to appropriately safeguard Canadian payload data. In our view, Google's actions following its discovery of Canadian payload data were justified, appropriate and sufficient to safeguard personal information collected in Canada. As such, we find that Google has satisfied the related safeguard provisions under the Act.
49. Google's counsel has stated that Canadian payload data shall remain secure until deleted, and that any third party requests to view that data will be resisted to the fullest extent possible by law. To this point, we note that several jurisdictions and laws are engaged in this matter – including laws of evidence – all of which must be taken into account in determining when to delete Canadian payload information.

## Conclusion

50. On October 15, 2010, our Office shared the preliminary findings of our investigation with Google and invited their response. Taking into consideration their response, we have revised our preliminary letter of findings. What follows is a summary of our latest findings and recommendations.
51. Google is a recognized leader in information management and, by its own admission, a company which pursues ideas that sometimes push the limits of social norms and technologies. It is also a company of tremendous resources and expertise. As an industry leader, it owes a special responsibility to those whose personal information it uses for commercial purposes to ensure that its corporate innovations are balanced with appropriate levels of privacy protection.





52. In the case at hand, Google failed to live up to its own standards of transparency in the collection of personal information. The results of our investigation suggest that the collection of payload data was entirely avoidable. Had the company's own controls and compliance measures operated as they were intended, and had the company instilled a more robust privacy management framework, this incident is unlikely to have occurred. The personal information of Canadians collected would likely have remained unearthed, and Google's reputation for privacy would not have been so seriously affected.
53. In finding Google in contravention of the Act, we wish nonetheless to recognize and commend the company for the manner in which it handled the incident. But for the measures the company undertook to segregate and secure Canadian payload data, the ramifications of the incident in question could have been far more serious.
54. By all measures, the personal information collected from Canadian WiFi networks appears to have been appropriately safeguarded and is now pending destruction.
55. Google submits that it continues to design privacy protections into all of its products and services. It has also stated that its employees will continue to receive orientation and code-of-conduct training that includes a privacy and data-security component. In order to avoid a recurrence of this incident, Google has further committed to reviewing its product launch procedures, code review procedures and other such internal processes to ensure appropriate oversight for privacy concerns.
56. As of the issue date of this report, Google's review of its privacy procedures and policies was well underway.

### ***Recommendations***

57. The Office of the Privacy Commissioner of Canada shares Google's goal in avoiding a recurrence of this incident. In this regard, we are pleased that Google has accepted our recommendations to reduce the risk of any future such privacy violation.
58. To this end, we have encouraged the organization to ensure that any and all operational controls are complemented by an overarching governance model



embodying the privacy principles espoused by the Act. We have also asked Google to respect reasonable timelines in the implementation of both a privacy governance model and its revised processes and procedures.

59. After reviewing the additional information provided by Google to this Office on February 1, 2011, we have made the following recommendations:

- i. That Google re-examine and improve the privacy training it provides all its employees, with the goal of increasing staff awareness and understanding of Google's obligations under Canadian and international privacy laws.
- ii. That Google adopt a privacy governance model which ensures:
  - the effective implementation and operation of controls to ensure that the privacy impacts of programs, products and services are taken into account prior to their launch;
  - that qualified privacy personnel are designated and assigned in the review and approval process for Google products;
  - that senior management is held accountable for compliance with Google's obligations under privacy laws.
- iii. That Google delete the Canadian payload data collected, to the extent that Google is permitted under Canadian and U.S. laws. If the Canadian payload data cannot immediately be deleted, that data must continue to be properly safeguarded, with access to the data strictly limited.

### ***Response***

60. In response to our recommendations regarding privacy training, Google has stated that it will be significantly augmenting the privacy and security training provided to all of its employees, from new-hires to existing employees. The training program, which began in December 2010, will be rolled out across all functions within the organization and includes a renewed emphasis on Google's Privacy Principles (as well as employee obligations under the company's code of conduct).





61. According to Google's Code of Conduct, employees are responsible for understanding their obligations "to respect and protect the privacy" of users' personal information. As part of this obligation, all employees are required to participate in Code of Conduct training. Participation in this training is mandatory when joining Google and at two-year intervals thereafter.
62. In addition to the training mentioned above, Google has begun to implement new online training modules for all Google employees, some specifically addressing data security and privacy. The data security module began its pilot run in December of 2010, and is said to be currently undergoing final revisions for full deployment. Completion of these training modules will be mandatory for all employees and is to be tracked via Google's internal auditing tools.
63. Finally, Google will be offering five additional training programs specifically tailored to address privacy in the context of Google's Engineering, Product Management, People Operations, Sales and Legal functions. Google has indicated that since late 2010 a cross-functional team (drawing from Google's Engineering, Product Management, Business Operations, Privacy Counsel and Product Counsel teams) has been piloting training sessions for new employees joining Google's engineering or product management teams. Once launched, these training sessions will be led by engineers and product managers who have demonstrated leadership in privacy. Similar training modules will be developed and targeted towards other Google employees who handle personal data or are involved in Google's privacy efforts, including Google's legal team.
64. In response to our recommendation regarding privacy compliance governance, Google is said to be implementing a system for tracking all projects that collect, use or store personal information and for holding the engineers and managers responsible for those projects accountable for privacy.
65. In November of 2010, Google began requiring engineering project leaders ("Tech Leads") to draft, maintain, submit and update Privacy Design Documents for each and every project they are responsible for. If the project operates as intended, it will ensure mandatory privacy documentation for user-facing products, experimental projects, and services that are internal to Google. These documents should play an important role in ensuring that engineering and product teams assess the privacy impact of their products and services from inception through launch. Specifically, the Privacy Design Documents will require Google's Tech Leads to describe the types of



data that their projects collect, handle or process as well as how that data is to be protected. Privacy Design Documents are to be regularly reviewed by managers and will be considered during employee performance review cycles. Google expects the first set of manager reviews to occur in 2011.

66. To complement the Privacy Design Documents, Google will be relying on a number of processes to validate the information provided by Tech Leads, thus ensuring that privacy best practices are being observed. These processes centre around the work of Google's Privacy Review Team, Product Counsel, Privacy Counsel, and its Internal Audit Team. Google's Internal Audit Team will conduct periodic audits to verify the completion of selected Privacy Design Documents and their review by the appropriate managers. They will also lead quarterly audits of certain products to validate their privacy practices against identified controls.
67. Specifically in regards to its location-based services, Google is said to be piloting a cross-functional review process. Under this process, members of Google's Privacy Engineering, Product Counsel and Privacy Counsel teams have been reviewing proposals involving geolocation for collection activities, as well as the software programs that are to be used for the collection of data.
68. Lastly, in regards to the deletion of personal information, Google has reported that it has begun deleting the payload data identified as having been collected in Canada. As anticipated, this process has been complicated by the myriad of rules and regulations that the company is subject to under Canadian and U.S. law. As the deletion process continues, Google has assured our Office that no one, other than OPC investigators and those who facilitated their investigation, have accessed Canadian payload data (as identified). Until such time as the data can be fully destroyed, it shall remain segregated, secured, and unused.

#### *Follow-up*

69. All in all, our Office is satisfied that, once fully implemented, Google's proposed remedial measures as set out above will meet the privacy issues underscoring our recommendations.



70. However, our Office remains deeply concerned about this incident. We view Google's violations of the Act in these circumstances largely as a result of its failure to have implemented the proper policies and procedures to protect personal information. Indeed, as a matter of accountability, Google is not only responsible for the personal information it has under its control, but is required under the Act to have in place the policies and practices to give effect to the principles enshrined under the Act. Without ensuring that organizations under the Act also have the proper practices in place to protect personal information, the accountability principle would be reduced to being nothing but a hollow dictate.
71. The obligation that organizations must have in place the proper practices, as a matter of accountability, concords with a growing international recognition that the protection of personal information requires real and effective measures. It is this Office's view that organizations need to implement appropriate and effective measures to put into effect the principles and obligations of the Act, including effective compliance and training programs, as an essential part of ensuring that organisations remain accountable for the personal information they collect, use or disclose.
72. Given the importance of having the proper procedures and policies in place to give effect to the personal information protection measures enshrined under the Act, and their fallibility as this case clearly demonstrated, we are also requesting that Google undergo and share with us the results of an independent, third-party audit of its privacy programs within one year from the date of this report. It is our view that such an audit will help measure the effectiveness of Google's proposed measures vis-à-vis its overall privacy compliance regime.
73. Recognizing that fully implementing this Office's recommendations may take some time, our Office is providing Google with one year in which to do so. Our Office has a continuing interest in ensuring that Google implements the measures needed to bring it in full compliance with the Act. As such, over the next twelve months, our Office will be closely monitoring Google's implementation of our recommendations.
74. As evidence of our Office's continuing intention to pursue this matter, we will be following up with Google next year to gauge full implementation of our recommendations. At that time, we will determine whether and how best to pursue the matter in accordance with our authorities under the Act.



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

June 3, 2011

**CONFIDENTIAL TREATMENT REQUESTED**

*By E-mail*

Theresa Z. Cavanaugh  
Acting Chief, Hearings and Investigations Division  
Enforcement Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **File No. EB-10-IH-4055**

Dear Terry:

Thank you again for meeting on May 18 to discuss the Commission's remaining factual and legal questions regarding Google's prior collection of Wi-Fi information. At the meeting, we advised the Enforcement Bureau and the General Counsel that the U.S. Department of Justice ("Department") had informed Google that it had completed its review of potential violations of federal law, including unlawful interception of communications, and closed its investigation. Google recently received the Department's declination letter, and is pleased to provide a copy for your information.

Just as Google has done with the Commission, the company cooperated fully with the Department's inquiry, and the letter reflects the Department's recognition of the significant remedial efforts undertaken by Google to avoid any recurrence of the situation. Last fall the Federal Trade Commission also completed its inquiry and declined to take any action, again in large measure based on the facts Google provided and the remedial steps undertaken. Google continues to work towards closing the multi-state Attorney General inquiry into the matter, and has provided much the same information to the States as it has provided to the Commission. Given this history, Google trusts the information it has provided to the Commission will lead to a prompt resolution of its inquiry.

As Google's responses to the Bureau's Letter of Inquiry have made clear, Google viewed this incident as a teachable moment and has undertaken a comprehensive privacy program to ensure that it addresses privacy concerns, not only at the beginning of product development but throughout its lifecycle. Google has provided the Commission with a detailed description of these efforts. There may be other things that can be done to better educate consumers about wireless security in their home networks, [REDACTED]

[REDACTED]

Google also is following up on its offer to provide the code used by the engineer to extract the URL data, and separately the code that was used to extract MAC addresses for use in location services, as discussed at the May 18 meeting. (Due to ongoing litigation, however, the company is unable to provide any privileged reports regarding the code.)

Finally, since our last meeting, Canada's Office of Privacy has provided to Google its official findings, which we enclose. We re-confirm that no official English translations of the French and Dutch dispositions are available at this time.

In closing, Google believes the Bureau has had the critical facts before it for some time, and we now have had an opportunity to review the applicable law with the Bureau and the General Counsel. Because Google's passive collection of Wi-Fi information broadcast from networks configured to be readily accessible to the general public was lawful under Section 2511 of Title 18, there can be no actionable claim of interception under Section 705 of Title 47. Even though it was lawful, Google hopes it has conveyed that maintaining people's trust is crucial to everything Google does, and in this case, Google admittedly fell short. Just because it was lawful does not mean it was the right thing for Google to do.

Google looks forward to the Commission completing its inquiry promptly. If there are other questions Google can answer, please let us know.

---

<sup>1</sup> Pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, we request confidential treatment of this letter and enclosures. The information provided herewith falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. § 552(b)(4). *See also* 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905). This letter concerns the highly sensitive subject of the Street View Wi-Fi data collection, and the information herein customarily would be guarded from competitors. *See* 47 C.F.R. § 0.457(d)(2). Google has not made this information available to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and/or state attorneys general. Consistent with 47 C.F.R. § 0.459(d)(1), we request notification by the Commission if release of the enclosed redacted material is sought pursuant to FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

**Lampert, O'Connor & Johnston, P.C.**

FILE NO. EB-10-IH-4055 – CONFIDENTIAL TREATMENT REQUESTED

June 3, 2011

Page 3

Sincerely,

A handwritten signature in black ink, appearing to read "E. Ashton Johnston", with a long horizontal flourish extending to the right.

E. Ashton Johnston  
*Counsel to Google Inc.*

Enclosures

cc: Austin Schlick, General Counsel (by e-mail)  
[REDACTED] Investigations and Hearings Division, Enforcement Bureau (by e-mail)







I, [REDACTED] for Google Inc. ("Google"). I make this declaration based on personal knowledge as to the truth of the facts stated herein.

1. I understand that the States have been provided with a detailed report by the independent technical consulting firm, Stroz Friedberg, which confirmed Google's statements that in addition to WiFi network information such as MAC address and SSID, payload data broadcast publicly from unencrypted networks was stored on disks in the vehicles while payload from encrypted networks was discarded. The WiFi data was later copied from the disks at a Google data center and stored on Google's file servers ("GFS") unparsed and in its raw form.
2. Google has determined that the payload data was accessed once. The engineer who wrote the gstreamer code wrote a script to access the payload data to extract a sampling of any URLs present. The process was automated and did not involve or require human review of the overall payload contents. The engineer viewed resulting URLs, determined that there was no useful purpose for the data, and discarded them. Google has determined that the engineer did not access the payload data again.
3. When Google confirmed the first week of May 2010 that the collection of payload had in fact occurred, it immediately stopped driving its Street View vehicles. I, myself, did not know about the payload data collection until May 2010 and [REDACTED] May 14, 2010 blog post on the subject that publicly informed Google users and governmental agencies around the world of this issue.
4. Google located the directories where the WiFi data was stored and confirmed that payload data indeed was present and being stored in GFS in an unparsed form. Google also searched its entire code repository for any code that would have accessed the payload data or referenced the storage format used for the payload, and confirmed that the payload was not being used in any product or service. As you know, Google has confirmed to you, and publicly, that the payload data has not been used in any product or service, and has not been shared with any unauthorized person or third party, nor is Google aware of any unauthorized access to the data.
5. With respect to the collected payload data, Google segregated and secured the payload data onto a disk that is disconnected from Google's network and is inaccessible to others. The data for the United States was further segregated, encrypted and remains securely stored.

I declare that the above information is true and correct.

[REDACTED]

Signed this 7th day of June 2011 at Mountain View, California.



1 WSGT

- W S G T

12

18 孰孰 18 孰孰 18 孰孰

18 孰孰 18 孰孰 18 孰孰

18 孰孰 18 孰孰 18 孰孰



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

May 16, 2011

**CONFIDENTIAL TREATMENT REQUESTED**

*By E-mail*

Theresa Z. Cavanaugh  
Acting Chief, Hearings and Investigations Division  
Enforcement Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **File No. EB-10-IH-4055**

Dear Terry:

We look forward to our meeting this week, at which we hope to resolve any outstanding factual and legal questions the Bureau may have regarding the above-referenced matter.

The Bureau previously asked whether any patent applications have been filed and/or patents issued associated with the software used for the Wi-Fi data collection program at issue. We responded that no such applications had been made.

There are no patents associated with the Wi-Fi data collection program.

Also at our meeting on April 27, the Bureau asked for English language translations of the dispositions of the French and Dutch inquiries, if available. We confirm that no official English translation of either disposition is available at this time. The Bureau also asked about Canada's resolution and we can advise that the Commissioner has not yet released her final opinion.

**Lampert, O'Connor & Johnston, P.C.**

FILE NO. EB-10-IH-4055 - CONFIDENTIAL TREATMENT REQUESTED

May 16, 2011

Page 2

We trust this responds to your questions, and we look forward to resolving any remaining questions you may have on May 18.<sup>1</sup>

Sincerely,



E. Ashton Johnston  
*Counsel to Google Inc.*

cc: Mindy Littell, Investigations and Hearings Division, Enforcement Bureau (by e-mail)

---

<sup>1</sup> Pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, we request confidential treatment of this letter. The information herein falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. § 552(b)(4). *See also* 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905). This letter concerns the highly sensitive subject of the Street View Wi-Fi data collection, and the information herein customarily would be guarded from competitors. *See* 47 C.F.R. § 0.457(d)(2). Google has not made this information available to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and/or state attorneys general. Consistent with 47 C.F.R. § 0.459(d)(1), we request notification by the Commission if release of the enclosed redacted material is sought pursuant to FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.





u wsg

W S G R

p6

t x <sup>2</sup> t x t

t x t ( t x )

d o c x d o



**DECLARATION OF** [REDACTED]

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]
2. I have personal knowledge of the representations that the Company has made in its Responses to P. Michelle Ellison, Chief of the Federal Communications Commission Enforcement Bureau, including the representations made in the Company's November 1, 2011, letter to the Bureau, and hereby verify the truth, accuracy and completeness of the same.
3. The Company has conducted a comprehensive search for relevant materials in its possession, including emails, in response to the Bureau's requests.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 5, 2011.

[REDACTED]



**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 18-46**

**CONFIDENTIAL**

[REDACTED]

Subject: (Lebowski-tech) a code review (5557508) Add a dashboard for in-car testing. The intended audience

Hello [REDACTED]

I'd like you to do a code review. Please execute

[REDACTED]

[REDACTED]

to review the following code:

[REDACTED]

CONFIDENTIAL





**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

November 1, 2011

*By Hand Delivery*

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google" or the "Company"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of the enclosed letter responding to the October 21, 2011 letter to Google from Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau, in the above-referenced matter. As shown below, the responses contain information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential."<sup>1</sup>

Responses to Items 15 and 16. The redacted portions of Google's response to Items 15 and 16 contain specific information regarding Google's private business and internal operations. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties and has established procedures to protect such commercially sensitive and personal information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Item 17. The redacted portions of Google's response to Item 17, and Documents 17B-1, 17C-1, 17C-2, and 17C-3 contain highly confidential and contain competitively sensitive information that "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). The Documents identify Company employees (including their authors

---

<sup>1</sup> 5 U.S.C. § 552(b)(4).

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment – File No. EB-10-IH-4055

November 1, 2011

Page 2

and references to other Google personnel), reflect their authors' subjective thoughts and analysis, and contain internal Company discussions of trade secrets, including detailed information about and insight into Google's internal business processes (design, code, logging, testing, monitoring, documentation, and work flow), all of which is proprietary to Google. Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive and personal information internally, and has not publicly disclosed these documents or their contents. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the documents and the information they contain relate to business and operations of Google. See 47 C.F.R. § 0.459(a)(4). Documents 17B-1, 17C-1, 17C-2, and 17C-3 also contain personally identifying information about Google employees that "could reasonably be expected to constitute an unwarranted invasion of personal privacy." *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Response to Item 18. The redacted portions of Google's response to Item 18 and Documents 18-1 through 18-46 contain highly confidential and contain competitively sensitive information that "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). The Documents identify Company employees (including their authors and references to other Google personnel), reflect their authors' subjective thoughts and analysis, and contain internal Company discussions of trade secrets, including detailed information about and insight into Google's internal business processes (product design, development, testing, and launch, computer code, documentation, and work flow), all of which is proprietary to Google. Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive and personal information internally, and has not publicly disclosed these documents or their contents. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the documents and the information they contain relate to business and operations of Google. See 47 C.F.R. § 0.459(a)(4). Documents 18-1 through 18-46 also contain personally identifying information about Google employees that "could reasonably be expected to constitute an unwarranted invasion of personal privacy." *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Response to Item 19. The redacted portion of Google's response to Item 19 contains information about the Company's knowledge regarding specific Company documents. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2).

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment – File No. EB-10-IH-4055

November 1, 2011

Page 3

We enclose herewith both a complete, unredacted copy of this submission, to be treated as confidential, and a separate copy marked REDACTED. Consistent with 47 C.F.R. § 0.459(d)(1), Google requests notification by the Commission if release of the redacted material in the Letter is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
Joseph A. Bissonnette  
*Counsel to Google Inc.*

Enclosures

cc: Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau (by email)  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau (by email)



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

September 7, 2011

*By Hand Delivery*

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **AMENDED REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, and to the August 18, 2011 letter from P. Michele Ellison, Chief, Enforcement Bureau, Federal Communications Commission (the "Letter"), hereby submits this amended request for confidential treatment. As requested in the Letter, Google has reexamined all of its previously submitted narrative and documentary responses (collectively, the "Responses") to the November 3, 2010, letter to Google from P. Michele Ellison, Chief, Enforcement Bureau, Federal Communications Commission (the "LOI") and to the March 30, 2011, letter to Google from Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau, Federal Communications Commission (the "Supplemental LOI"), as well as prior requests for confidential treatment submitted concurrently with those Responses.

As a result of its reexamination of the Responses, Google has determined that additional narrative portions of Google's (1) December 10, 2010 responses to the LOI and (2) April 14, 2011 responses to the Supplemental LOI are not subject to confidential treatment. Accordingly, we submit herewith revised redacted copies of each of these three prior submissions. In addition, Google has determined that it has no revisions to its December 14, 2010 Supplement to Responses to the LOI (filed December 14, 2010), December 20, 2010 Second Supplement to Responses to the LOI (filed December 20, 2010), or April 28, 2011 Further Response to the Supplemental LOI.

Below we address Responses to each numbered request in the LOI and the Supplemental LOI for which confidential treatment is requested. As shown below, portions of these Responses contain information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"),

which provides a statutory basis for withholding from public inspection “matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential,”<sup>1</sup> and/or within Exemption 7(C), which provides a statutory basis for withholding from public inspection information compiled for law enforcement purposes and that “could reasonably be expected to constitute an unwarranted invasion of personal privacy.”<sup>2</sup>

**Revised Request for Confidential Treatment of December 10, 2010 Responses to the LOI**

LOI Response No. 2. The redacted portions of the Response contain sensitive and detailed information regarding Google’s private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection and the company’s internal review and actions taken in response to the matters that have evolved. This information “would customarily be guarded from competitors.” *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 3. The redacted portion of the Response contains sensitive and detailed information regarding Google’s private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information “would customarily be guarded from competitors.” *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 4. The redacted portions of the Response contain sensitive and detailed information regarding Google’s private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company’s internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google’s internal decisional processes “which would customarily be guarded from competitors.”

---

<sup>1</sup> 5 U.S.C. § 552(b)(4). *See also* 47 C.F.R. 0.457(d) (records not routinely available for public inspection include “trade secrets and commercial or financial information obtained from any person and privileged or confidential” under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

<sup>2</sup> 5 U.S.C. § 552(b)(7)(C). *See also* 47 C.F.R. 0.457(g)(3).



**Lampert, O'Connor & Johnston, P.C.**

Amended Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 3

*See* 47 C.F.R. § 0.457(d)(2). Further, the Response includes trade secrets such as descriptions of the processes by which Google creates and produces such products as Google Maps and Google's related geolocation server, which is highly confidential and competitively sensitive information. Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 5. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, the company's internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Further, the Response includes trade secrets such as descriptions of the processes by which Google creates and produces such products as Google Maps and Google's related geolocation server, which is highly confidential and competitively sensitive information. Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 6. The redacted portion of the Response contains sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 7. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection and the company's internal review and procedures taken in response to the matters that have evolved. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which

Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 8. The redacted portion of the Response contains sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company's internal review and actions, including its internal regulatory compliance procedures and actions. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 9. *See* Revised Request for Confidential Treatment of December 14, 2010 Supplement to Responses to the LOI, below.

LOI Response No. 10. The redacted portions of the Response contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. The information includes Google's internal decisional processes "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Further, the Response includes trade secrets such as descriptions of the processes by which Google creates and produces products, which is highly confidential and competitively sensitive information. Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

LOI Response No. 11. Documents 11-1, 11-2, 11-3, and 11-5 are confidential and proprietary documents that contain sensitive and detailed information regarding Google's private business and internal operational actions and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. We note that Documents 11-1, 11-2, and 11-3 were submitted with Google's December 10, 2010 Responses to the LOI and that revised versions were re-submitted on April 14, 2011; this request for confidential treatment extends to both submissions.

Documents 11-1 and 11-2 are the gstumbler and gslite project design documents and are proprietary to Google. They identify their author as a Google employee, contain references to other Google personnel, and reflect their author's subjective thoughts, analysis, and interpretation of how to carry out Wi-Fi data collection, which include the project's Objectives and Caveats (including security considerations and privacy considerations). Further, they contain trade secrets, including detailed information about and insight into Google's proprietary



**Lampert, O'Connor & Johnston, P.C.**

Amended Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 5

internal business processes (design, code, logging, testing, monitoring, billing and tax, documentation, work flow, and launch plans; patents; and document creation and review). Thus, these documents do not merely explain the functionality of technology or publicly available code or contain objective analysis of the project.

Documents 11-1 and 11-2 are highly confidential and contain competitively sensitive information that “would customarily be guarded from competitors.” *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive information internally, and has not publicly disclosed these documents or their contents. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the documents and the information they contain relate to business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4). Documents 11-1 and 11-2 also contain personally identifying information about Google employees that “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(7)(C); 47 C.F.R. 0.457(g)(3).

Document 11-3 contains computer code written by a Google employee and proprietary to Google. It contains all 25 files from the gstumbler code base, and collectively constitutes trade secrets. It also contains references to Google employees. The document is highly confidential and contains competitively sensitive information that “would customarily be guarded from competitors.” *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive and personal information internally, and has not publicly disclosed the document itself. Confidential treatment of the non-public portions of Document 11-3 is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the document and the redacted information in contains relates to Google’s business and operations. *See* 47 C.F.R. § 0.459(a)(4). Certain portions of Document 11-3 are non-confidential as a result of the public availability of the June 3, 2010 report by Stroz Friedberg, LLC (“Stroz”) (which Google provided on a non-confidential basis as Document 11-4 with its Responses to the LOI). Google does not object to the de-designation of such publicly available portions of Document 11-3, and will provide a redacted copy of that document promptly upon request. With respect to information contained in Document 11-3 that the Letter states is “derived from publicly available open-source software,” that derivation does not cause the entire software program, which remains proprietary to Google, subject to disclosure.

Document 11-5 is an independent report on an inspection of the Google Street View vehicles’ hardware and software capabilities conducted by Stroz, and on Google’s remediation efforts regarding the removal of Wi-Fi data collection capabilities. In a July 9, 2010 blog post, Google disclosed the fact that Stroz approved a protocol to ensure that any Wi-Fi related software is removed from Google’s Street View cars before they drive again. However, neither Document 11-5 nor any information in it have been publicly disclosed. The document contains information about Google’s remediation efforts and other company processes and procedures related to the Street View, including the actions of Google personnel. This is highly confidential and competitively sensitive information that “would customarily be guarded from competitors.”

*See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive information internally, and as noted has not publicly disclosed the document or its contents. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the documents and the information they contain relate to business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

**Revised Request for Confidential Treatment of December 14, 2010 Supplement to Responses to the LOI**

LOI Response No. 9. The redacted portions of Google's Response to Request No. 9, and Document 11-6, which is a confidential report prepared by Google regarding its collection of payload data using Street View cars and regarding the company's privacy assurance improvements, contain sensitive and detailed information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company's internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Further, the information contains trade secrets, including product design data, computer code, and descriptions of the processes by which Google creates and produces its products. This is highly confidential and competitively sensitive information that "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive information internally. Except for Appendix A and Appendix C to Document 11-6, Google has not made the information in Document 11-6 available to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and state attorneys general. Appendix A and Appendix C to Document 11-6 are being resubmitted on an unredacted basis. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to the business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4).

**Revised Request for Confidential Treatment of April 14, 2011 Responses to the Supplemental LOI**

Supplemental LOI Response No. 1. The redacted portions of Google's response to Supplemental Request No. 1 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, and the company's internal procedures for assuring regulatory compliance, personnel matters, and documentation. The information includes processes undertaken by Google to secure data and Google's internal decisional processes "which would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). The Response also includes highly confidential and competitively sensitive information concerning the processes by which Google creates and produces its products. Google does not routinely disclose such

information to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

Supplemental LOI Response No. 3. The redacted portion of Google's response to Supplement Request No. 3 contains detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

Supplemental LOI Response No. 4. The redacted portions of Google's response to Supplemental Request No. 4 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

Supplemental LOI Response No. 5. The redacted portions of Google's response to Supplemental Request No. 5 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

Supplemental LOI Response No. 6. The redacted portions of Google's response to Supplemental Request No. 5 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).



**Lampert, O'Connor & Johnston, P.C.**

Amended Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 8

Supplemental LOI Response No. 7. The redacted portions of Google's response to Supplemental Request No. 7 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4).

Supplemental LOI Response No. 8. The redacted portion of Google's response to Supplemental Request No. 8 contains detailed, specific information regarding Google's private business and internal operations, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has not publicly disclosed the employees' identities, and has established procedures to protect such commercially sensitive and personal information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google employees "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Supplemental LOI Response No. 9. The redacted portion of Google's response to Supplemental Request No. 9 contains detailed, specific information regarding Google's private business and internal operations, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has not publicly disclosed the employees' identities, and has established procedures to protect such commercially sensitive and personal information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google employees "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989) contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

**Lampert, O'Connor & Johnston, P.C.**

Amended Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 9

Supplemental LOI Response No. 11. The redacted portion of Google's response to Supplemental Request No. 11 contains detailed, specific information regarding Google's private business and internal operations, including the identity of Google employees. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has not publicly disclosed the employees' identities, and has established procedures to protect such commercially sensitive and personal information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google employees "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Supplemental LOI Response No. 12. The redacted portions of Google's response to Supplemental Request No. 12 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

Supplemental LOI Response No. 13. The redacted portions of Google's response to Supplemental Request No. 13 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

Supplemental LOI Response No. 14. The redacted portions of Google's response to Supplemental Request No. 14 contain detailed, specific information regarding Google's private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the

**Lampert, O'Connor & Johnston, P.C.**

Amended Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 10

Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

Documents 11-7 through 11-15 are confidential and proprietary documents that contain detailed, specific information regarding Google's private business and internal operational actions and decisions about the highly sensitive subject of the Street View Wi-Fi data collection, including the identity of Google employees.

Document 11-7, 11-8, 11-9, 11-10, 11-12, 11-13, and 11-15 are internal email communications, and Document 11-14 is an internal chat communication. They identify their authors, recipients, and other individuals as Google employees, and reflect their authors' subjective thoughts, analysis, and interpretation of how to carry out Wi-Fi data collection. Further, they contain trade secrets, including information about and insight into Google's proprietary internal processes and implementation of Street View. These documents and the information they contain, including personally identifying information, "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive and personal information internally, and has not disclosed these documents or their contents to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and/or state attorneys general. As noted above, Document 11-14 is an internal chat communication between Google employees. The fact of the existence of the communication may be public; however, neither the document nor the contents of the document has been disclosed to the public, or to third parties except as stated above. Confidential treatment of the documents is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the documents and the information they contain relate to business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4). Each of these documents contain personally identifying information about Google employees that "could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C); 47 C.F.R. 0.457(g)(3).

Document 11-11 is a project design document and is proprietary to Google. It identifies its author as a Google employee and reflect its author's subjective thoughts, analysis regarding project initiatives and implementation. It contains trade secrets, including detailed information about and insight into Google's proprietary internal business processes. Document 11-11 is highly confidential and contain competitively sensitive information that "would customarily be guarded from competitors." *See* 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive information internally, and has not disclosed the document or its contents to the public, or to third parties other than to a small number of officials of the Federal Trade Commission, the Department of Justice, and/or state attorneys general. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the documents and the information they contain relate to business and operations of Google. *See* 47 C.F.R. § 0.459(a)(4). Document 11-11 also contains personally identifying information about a Google employee that "could reasonably be expected to

**Lampert, O'Connor & Johnston, P.C.**

Amended Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 11

constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C); 47 C.F.R. 0.457(g)(3).

Google has made a good faith effort to identify materials that it has made public since its prior submissions. To be clear, Google does not consider the findings of foreign regulators, which Google may dispute, to result in a loss of confidential treatment for the materials identified as confidential.

Google believes it is necessary for the Commission to maintain the confidentiality of this information throughout the investigation and thereafter until it is destroyed. Consistent with 47 C.F.R. § 0.459(d)(1), Google requests notification by the Commission if release of the redacted material in the LOI Responses or the Supplemental Responses is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
Joseph A. Bissonnette  
*Counsel to Google Inc.*

Enclosures

cc: Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau (by email)  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau (by email)





**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

DOCUMENT 11-16

# GStumbler

Status: *Draft* (as of 2006-10-26)



## Contents

### Objective

### Background



### Privacy Considerations



## Objective

[\[Top\]](#)

We will gather Wi-Fi data as part of the Cityblock project's data acquisition. This data will be gathered just once and will be analyzed offline for use in other initiatives. The project is complete when all cityblock vehicles are equipped with Wi-Fi scanning equipment and have completed their work.

Analysis of the gathered data is a nongoal (though it will happen).

## Background

[\[Top\]](#)

TBD



[\[Top\]](#)



[\[Top\]](#)

[\[Top\]](#)



## Privacy Considerations

[\[Top\]](#)

The gathering of Wi-Fi data has a number of superficial privacy implications. A typical concern might be that we are logging user traffic along with sufficient data to

precisely triangulate their position at a given time, along with information about what they were doing. In reality this information is of little use, since the cityblock vehicle is not in proximity to any given user for an extended period of time.

None of the data gathered by GStumbler will be presented to end users of our services in raw form.

*TODO: discuss privacy considerations with the Product Counsel Team, and whether or not your privacy policy has been reviewed by Product Counsel.*

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)



*This document is Google Confidential.*



**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-17**

# GStumbler

Status: *Draft* (as of 2006-10-26)



## Contents

### Objective

### Background



### Privacy Considerations



## Objective

[\[Top\]](#)

We will gather Wi-Fi data as part of the Cityblock project's data acquisition. This data will be gathered just once and will be analyzed offline for use in other initiatives. The project is complete when all cityblock vehicles are equipped with



Wi-Fi scanning equipment and have completed their work.

Analysis of the gathered data is a nongoal (though it will happen).

## Background

[\[Top\]](#)

Data from Wardriving can be used a number of ways. The following is by no means exhaustive:

- to provide geolocation of Wi-Fi enabled users
- to determine market penetration of Wi-Fi
- to determine where Wi-Fi access is lacking
- to observe typical Wi-Fi usage snapshots

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)



[\[Top\]](#)

[REDACTED]

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]

## Privacy Considerations

[\[Top\]](#)

The gathering of Wi-Fi data has a number of superficial privacy implications. A typical concern might be that we are logging user traffic along with sufficient data to precisely triangulate their position at a given time, along with information about what they were doing. In reality this information is of little use, since the cityblock vehicle is not in proximity to any given user for an extended period of time.

None of the data gathered by GStumbler will be presented to end users of our services in raw form.

*TODO: discuss privacy considerations with Product Counsel.*

[REDACTED]

[\[Top\]](#)

[REDACTED]

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)

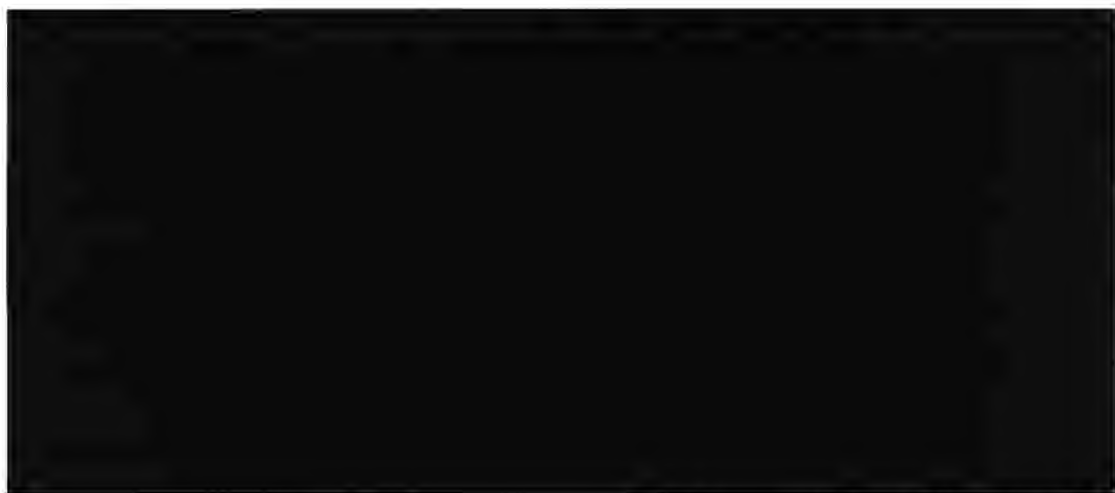
[REDACTED]

[\[Top\]](#)

[REDACTED]

[\[Top\]](#)

[REDACTED]



*This document is Google Confidential.*



**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-18**

# GStumbler

Status: *Draft* (as of 2006-10-26)



## Contents

### Objective

### Background



### Privacy Considerations



## Objective

[\[Top\]](#)

We will gather Wi-Fi data as part of the Cityblock project's data acquisition. This data will be gathered just once and will be analyzed offline for use in other initiatives. The project is complete when all cityblock vehicles are equipped with Wi-Fi scanning equipment and have completed their work.

Analysis of the gathered data is a nongoal (though it will happen).

## Background

[\[Top\]](#)

Data from Wardriving can be used a number of ways. The following is by no means

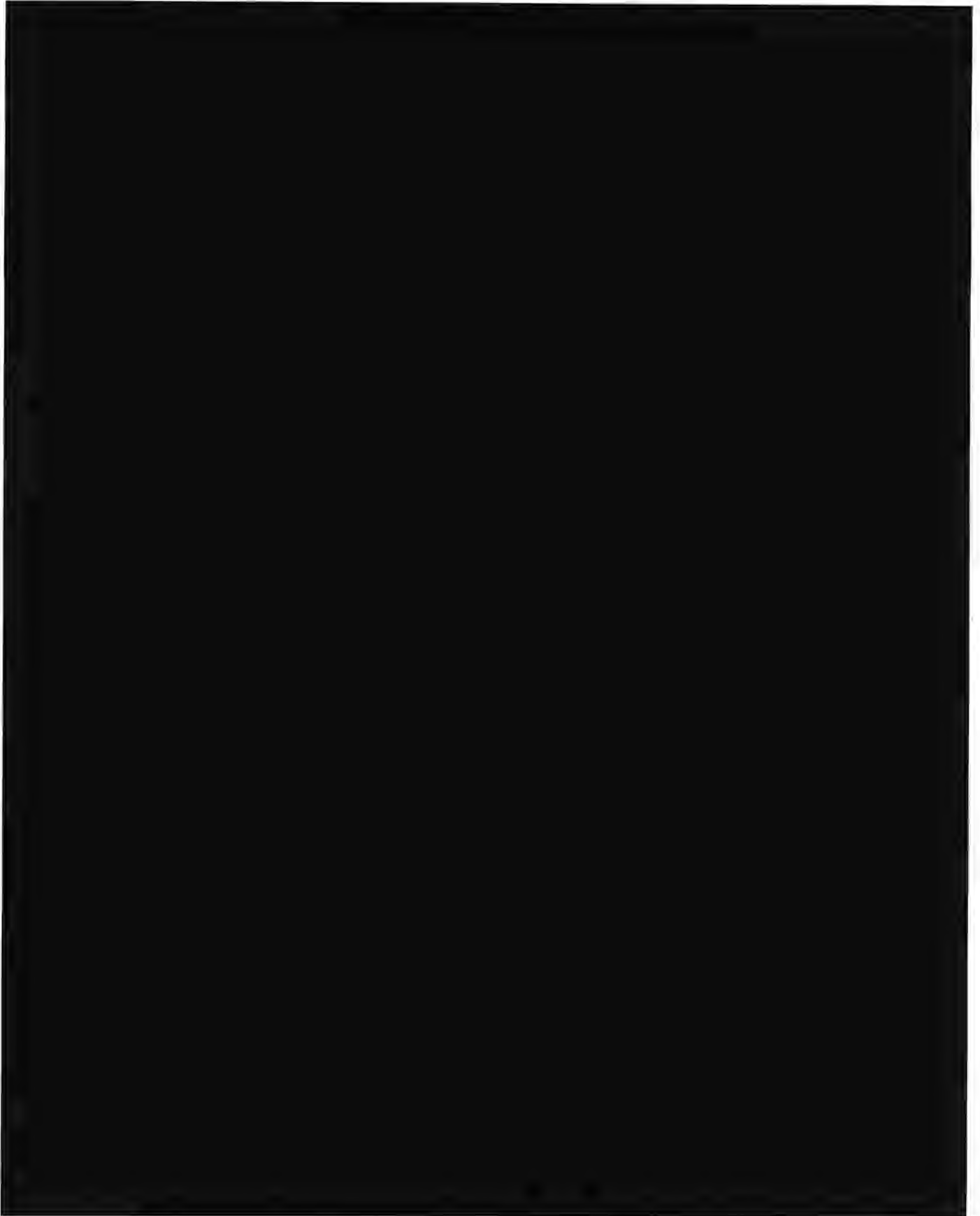


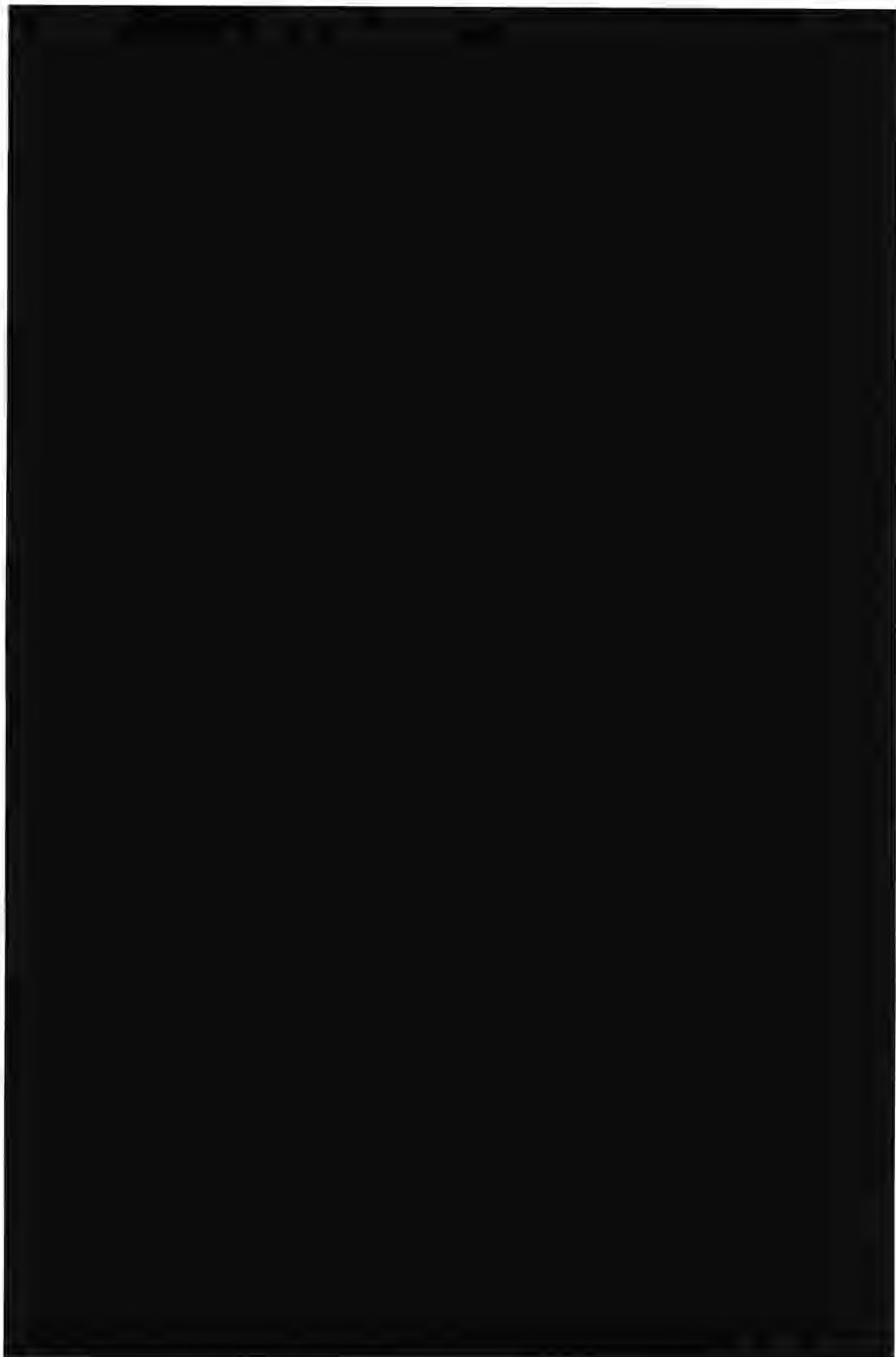
exhaustive:

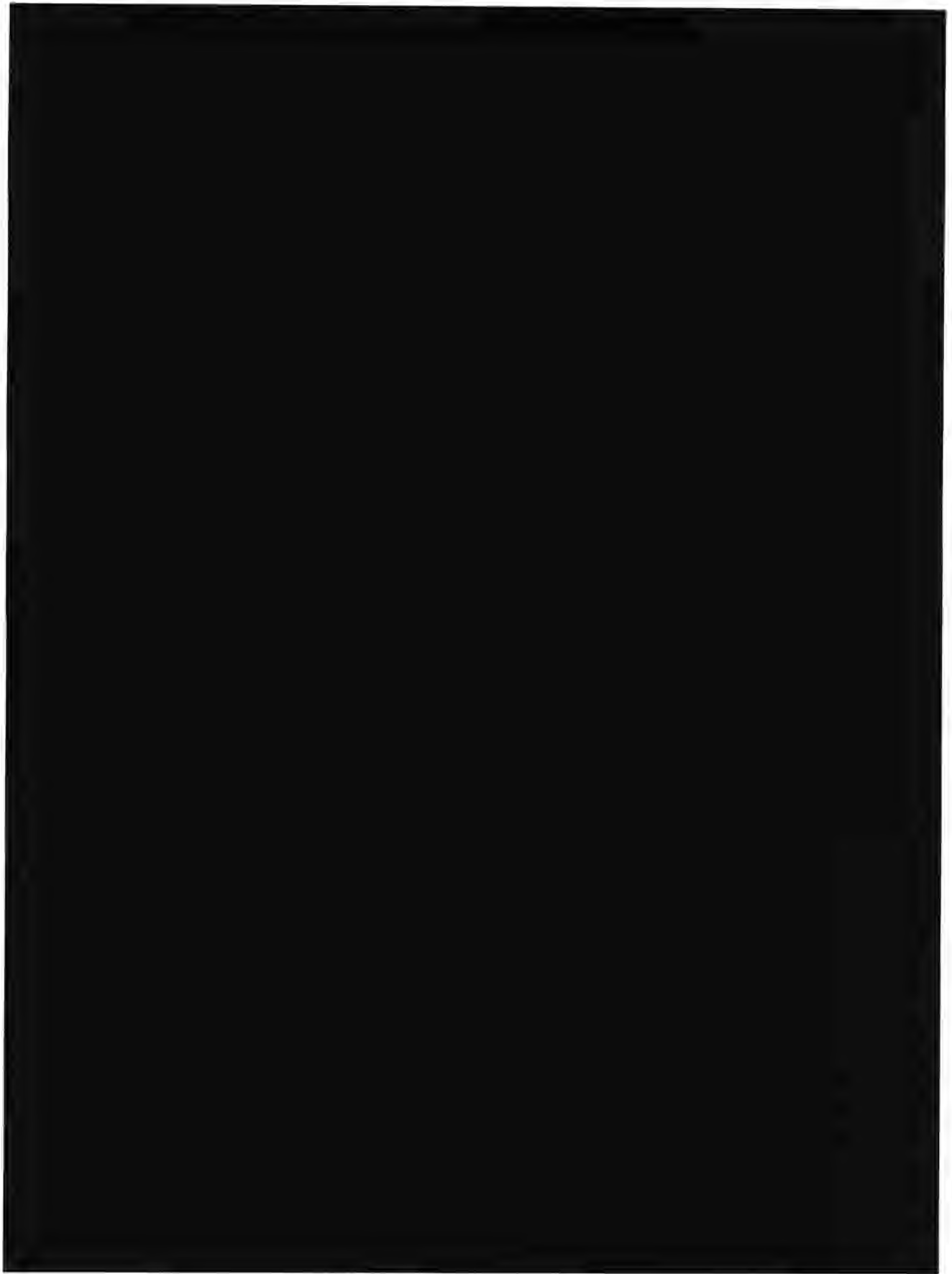
- to provide geolocation of Wi-Fi enabled users
- to determine market penetration of Wi-Fi
- to determine where Wi-Fi access is lacking
- to observe typical Wi-Fi usage snapshots

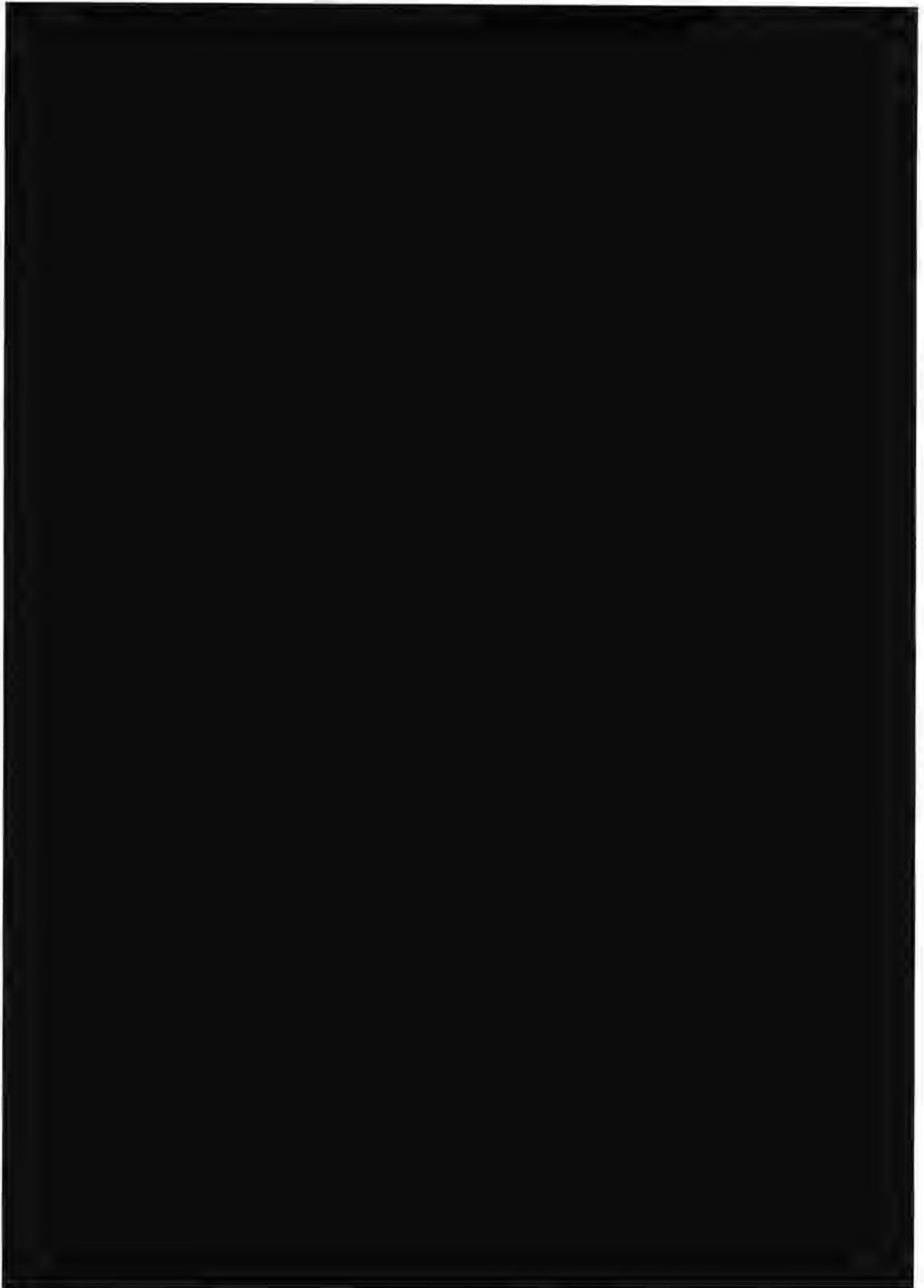
[Top]

[Top]









[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]



## Privacy Considerations

[\[Top\]](#)

The gathering of Wi-Fi data has a number of superficial privacy implications. A typical concern might be that we are logging user traffic along with sufficient data to precisely triangulate their position at a given time, along with information about what they were doing. In reality this information is of little use, since the cityblock vehicle is not in proximity to any given user for an extended period of time.

None of the data gathered by GStumbler will be presented to end users of our services in raw form.

*TODO: discuss privacy considerations with Product Counsel.*



[\[Top\]](#)



[\[Top\]](#)



[\[Top\]](#)



[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)



[\[Top\]](#)

[\[Top\]](#)

*This document is Google Confidential.*





**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-19**

# GStumbler

Status: *Draft* (as of 2006-10-26)



## Contents

### Objective

### Background



### Privacy Considerations



## Objective

[\[Top\]](#)

We will gather Wi-Fi data as part of the Cityblock project's data acquisition. This data will be gathered just once and will be analyzed offline for use in other initiatives. The project is complete when all cityblock vehicles are equipped with Wi-Fi scanning equipment and have completed their work.

Analysis of the gathered data is a nongoal (though it will happen).

## Background

[\[Top\]](#)

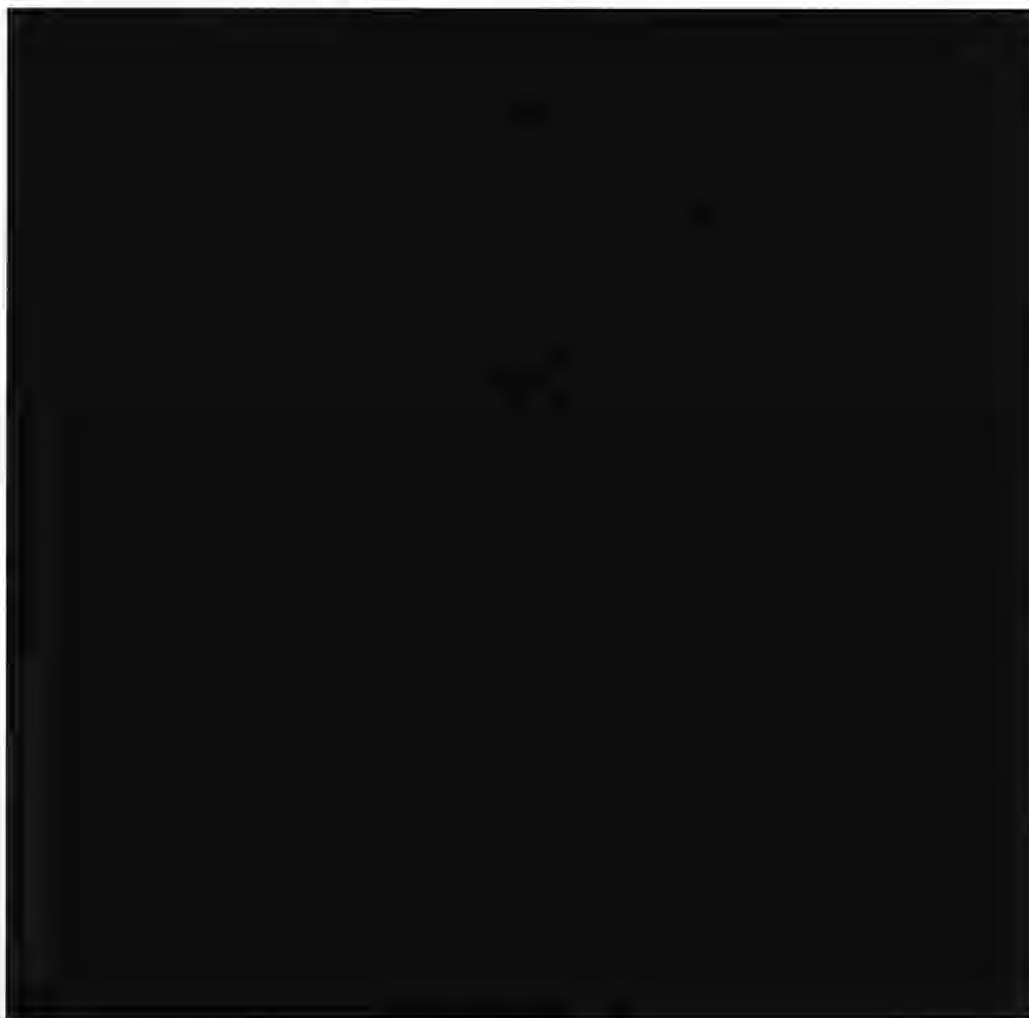
Data from Wardriving can be used a number of ways. The following is by no means

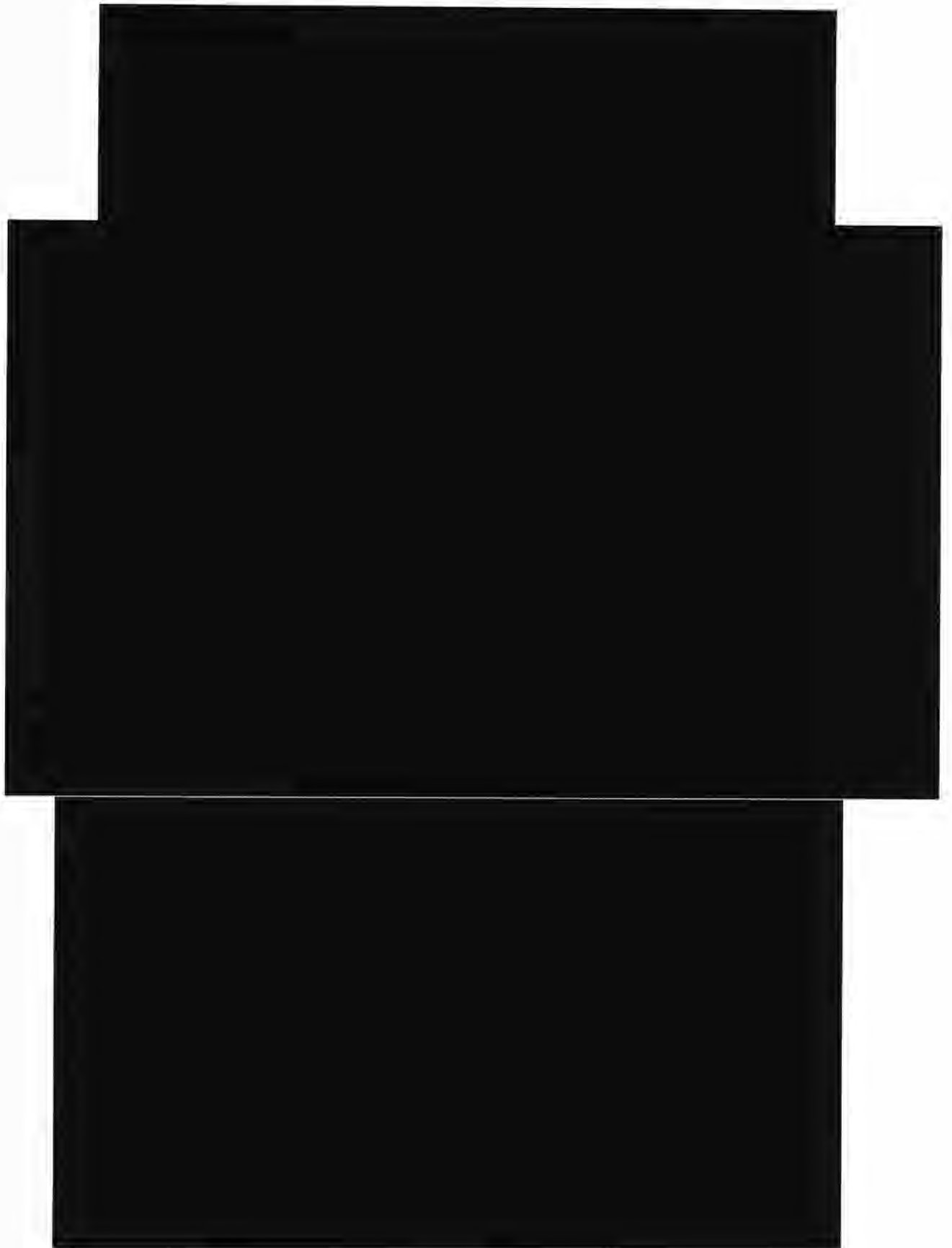
exhaustive:

- to provide geolocation of Wi-Fi enabled users
- to determine market penetration of Wi-Fi
- to determine where Wi-Fi access is lacking
- to observe typical Wi-Fi usage snapshots



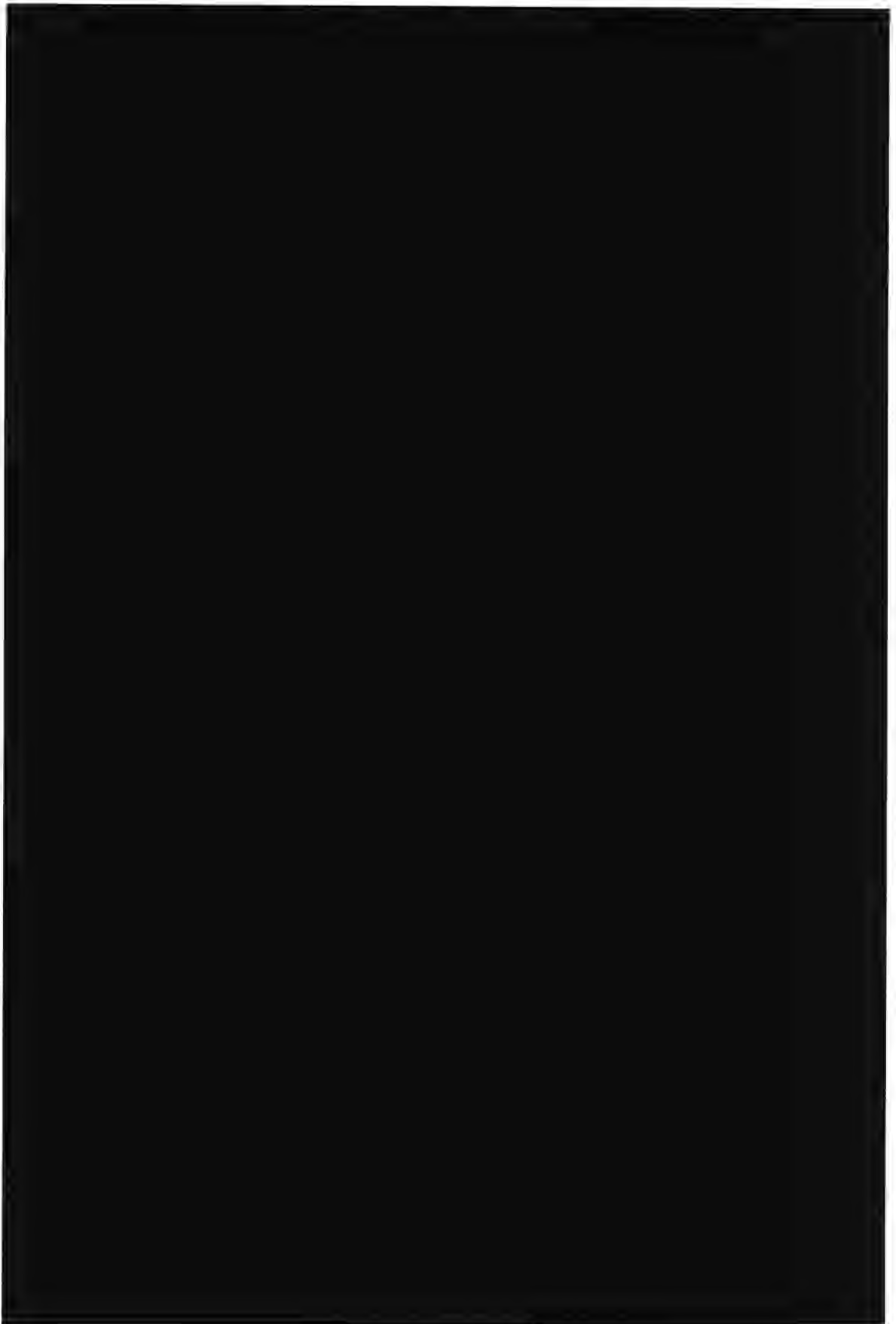
Top



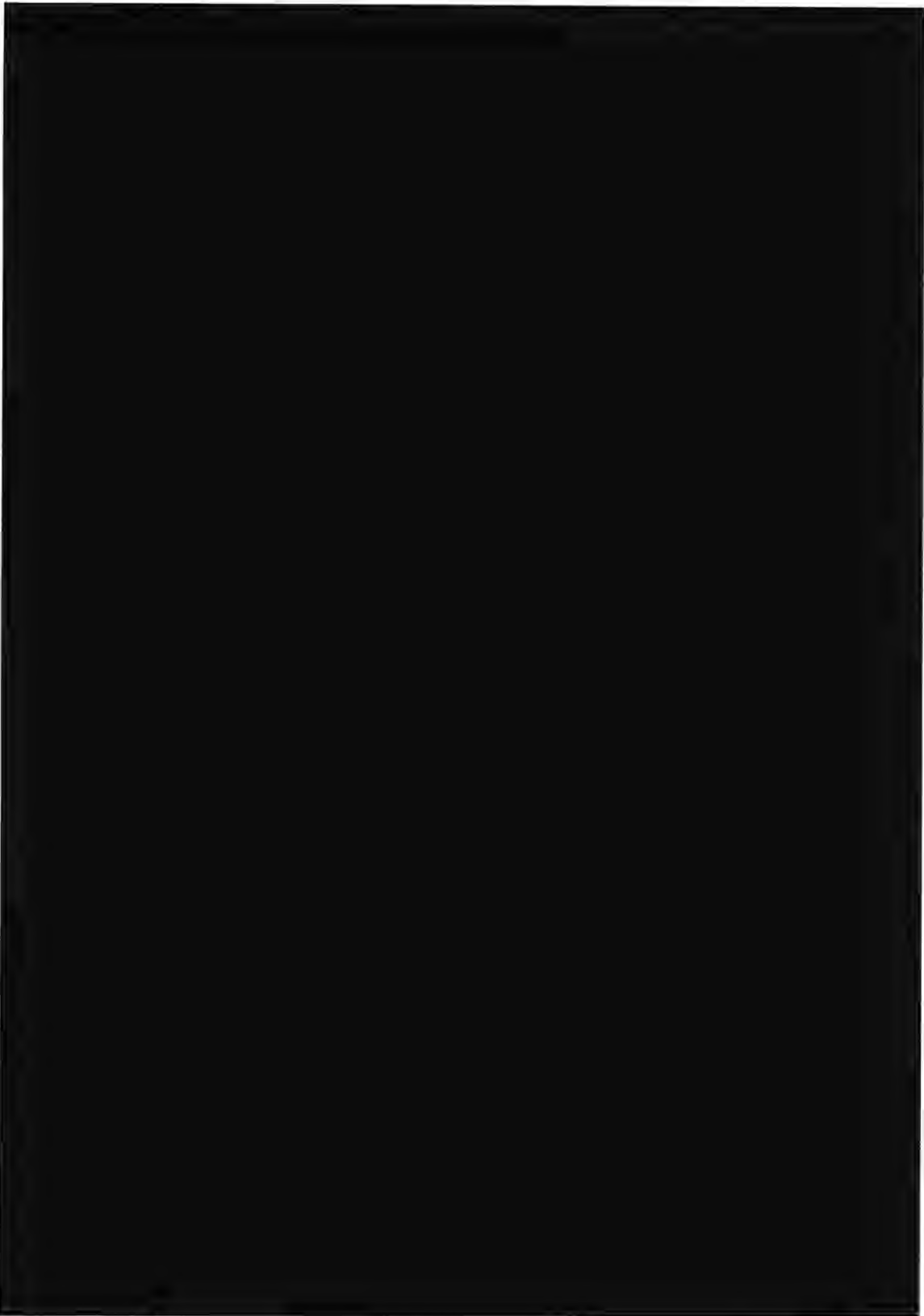












[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]



## Privacy Considerations

[\[Top\]](#)

The gathering of Wi-Fi data has a number of superficial privacy implications. A typical concern might be that we are logging user traffic along with sufficient data to precisely triangulate their position at a given time, along with information about what they were doing. In reality this information is of little use, since the cityblock vehicle is not in proximity to any given user for an extended period of time.

None of the data gathered by GStumbler will be presented to end users of our services in raw form.

*TODO: discuss privacy considerations with Product Counsel.*



[\[Top\]](#)



[\[Top\]](#)



[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[REDACTED]

[REDACTED]

[\[Top\]](#)

[\[Top\]](#)

[REDACTED]



*This document is Google Confidential.*



**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

DOCUMENT 11-20

# GStumbler

Status: *Draft* (as of 2006-10-26)



## Contents

### Objective

### Background



### Privacy Considerations



## Objective

[Redacted]

We will gather Wi-Fi data as part of the Cityblock project's data acquisition. This data will be gathered just once and will be analyzed offline for use in other initiatives. The project is complete when all cityblock vehicles are equipped with Wi-Fi scanning equipment and have completed their work.

Analysis of the gathered data is a nongoal (though it will happen).

## Background

[Redacted]



Data from Wardriving can be used a number of ways. The following is by no means exhaustive:

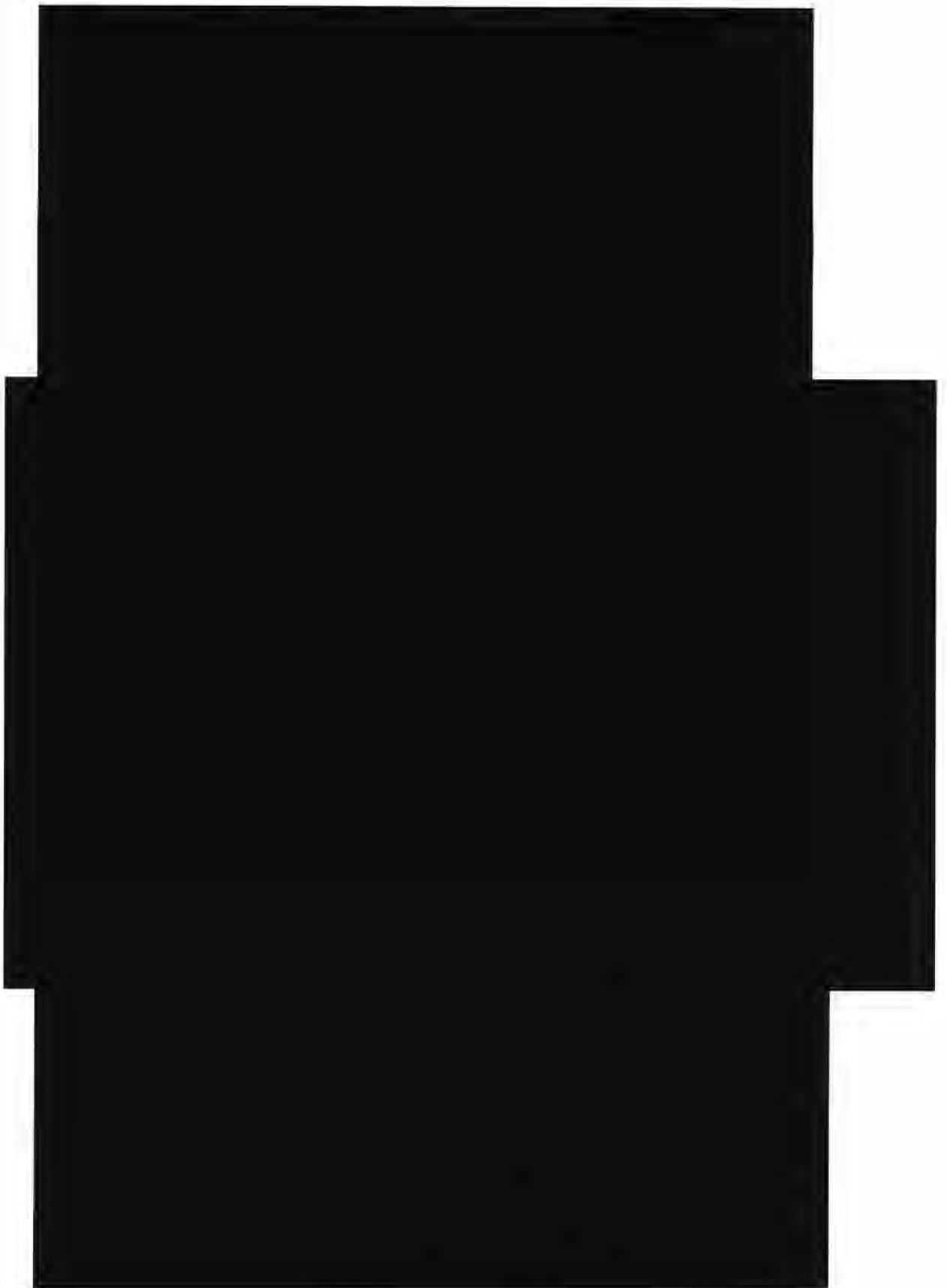
- to provide geolocation of Wi-Fi enabled users
- to determine market penetration of Wi-Fi
- to determine where Wi-Fi access is lacking
- to observe typical Wi-Fi usage snapshots

## Overview

[Top]

The open-source *Kismet* software will be used to scan for Wi-Fi frames. Specifically, *kismet\_drone* will run on commodity Wi-Fi hardware inside the Cityblock vehicle, with a connection to an antenna on the outside. The data from *kismet\_drone* stream over the Cityblock vehicle's network to *gstumbler*, which will coexist with the vehicle's Data Acquisition Subsystem. *gstumbler* will be under control of the vehicle's Process Controller, will collect location information from the GPS Logger, and will write its own log file.

[Top]



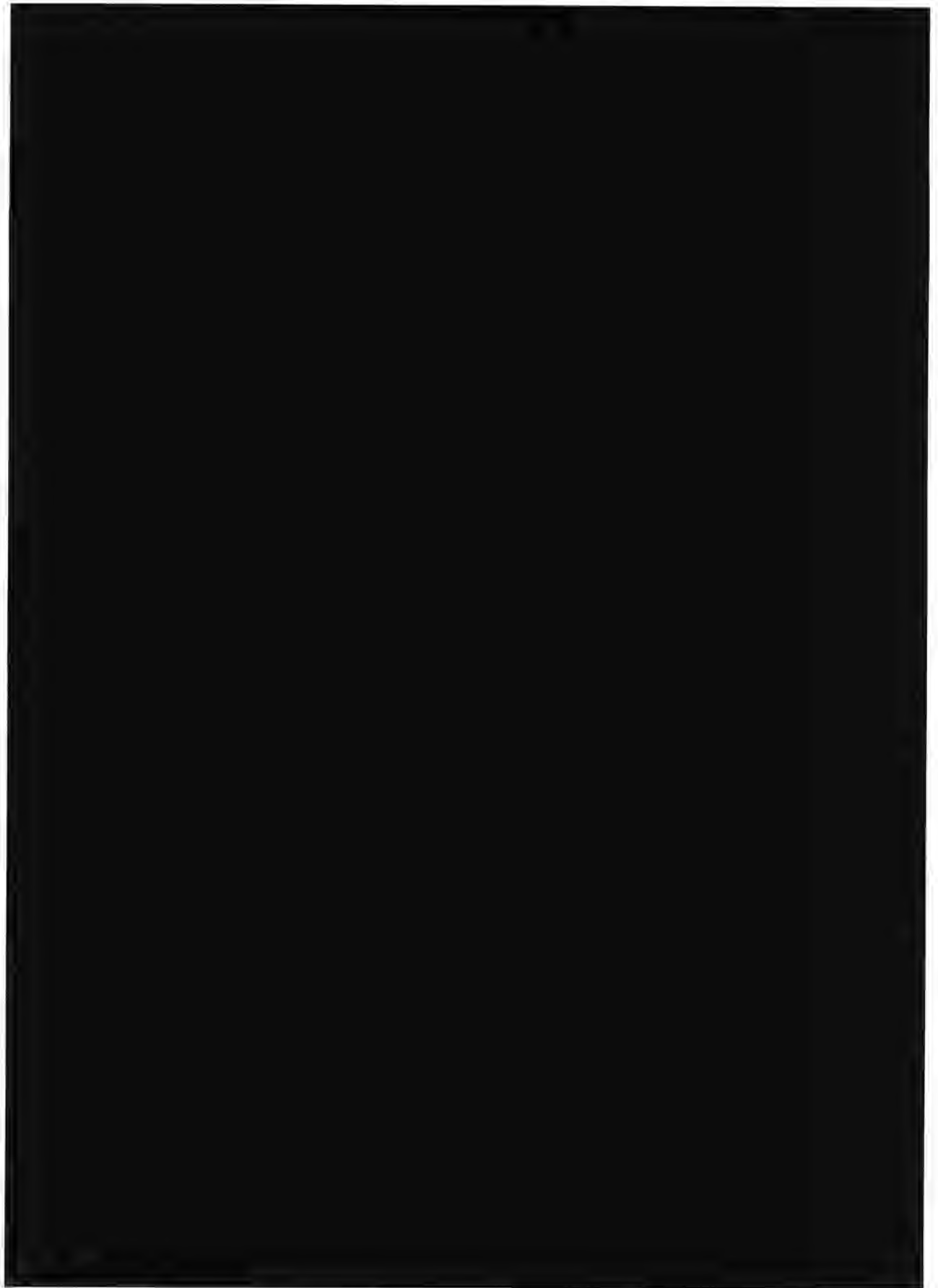


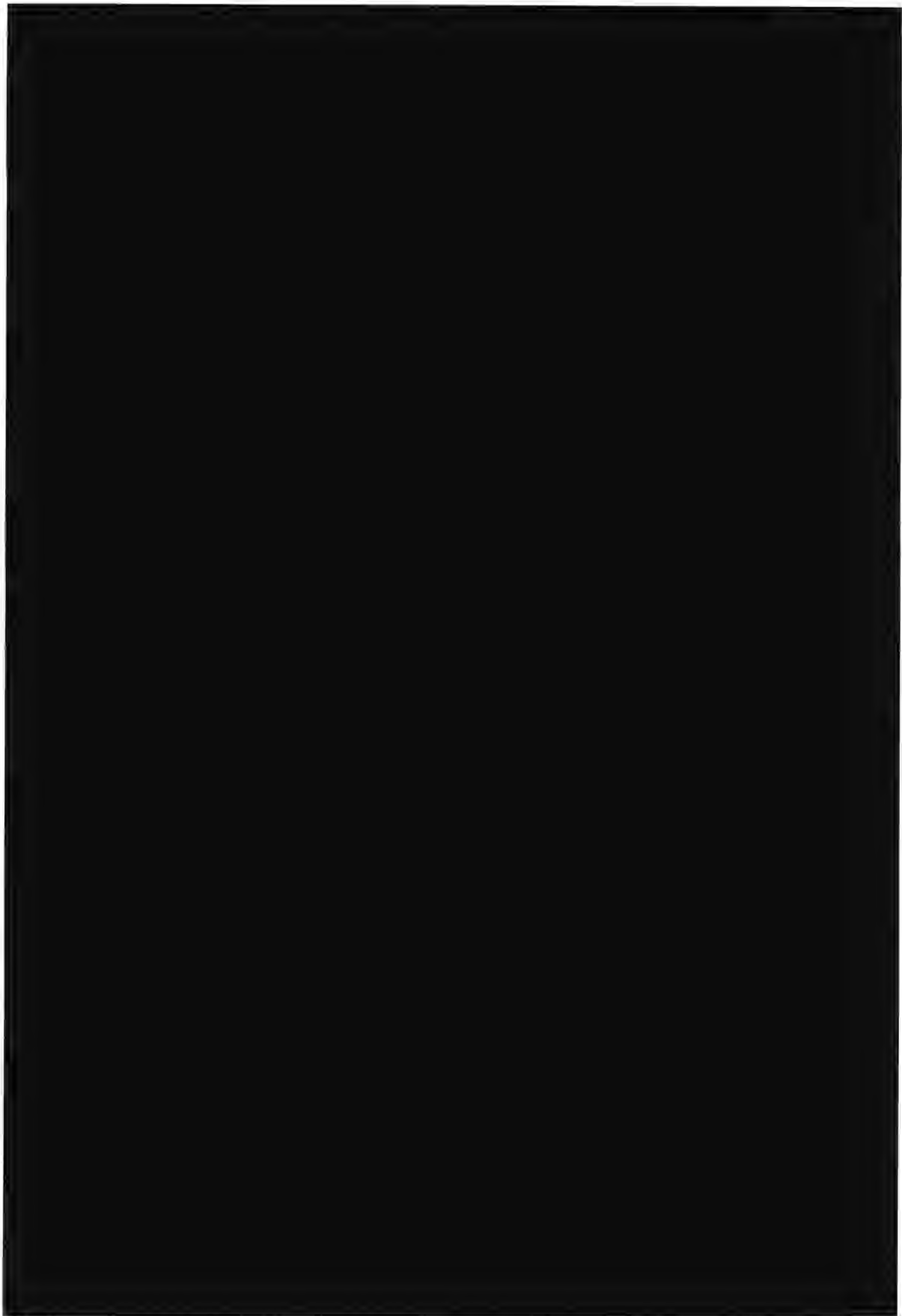


[REDACTED]

[REDACTED]











## Privacy Considerations

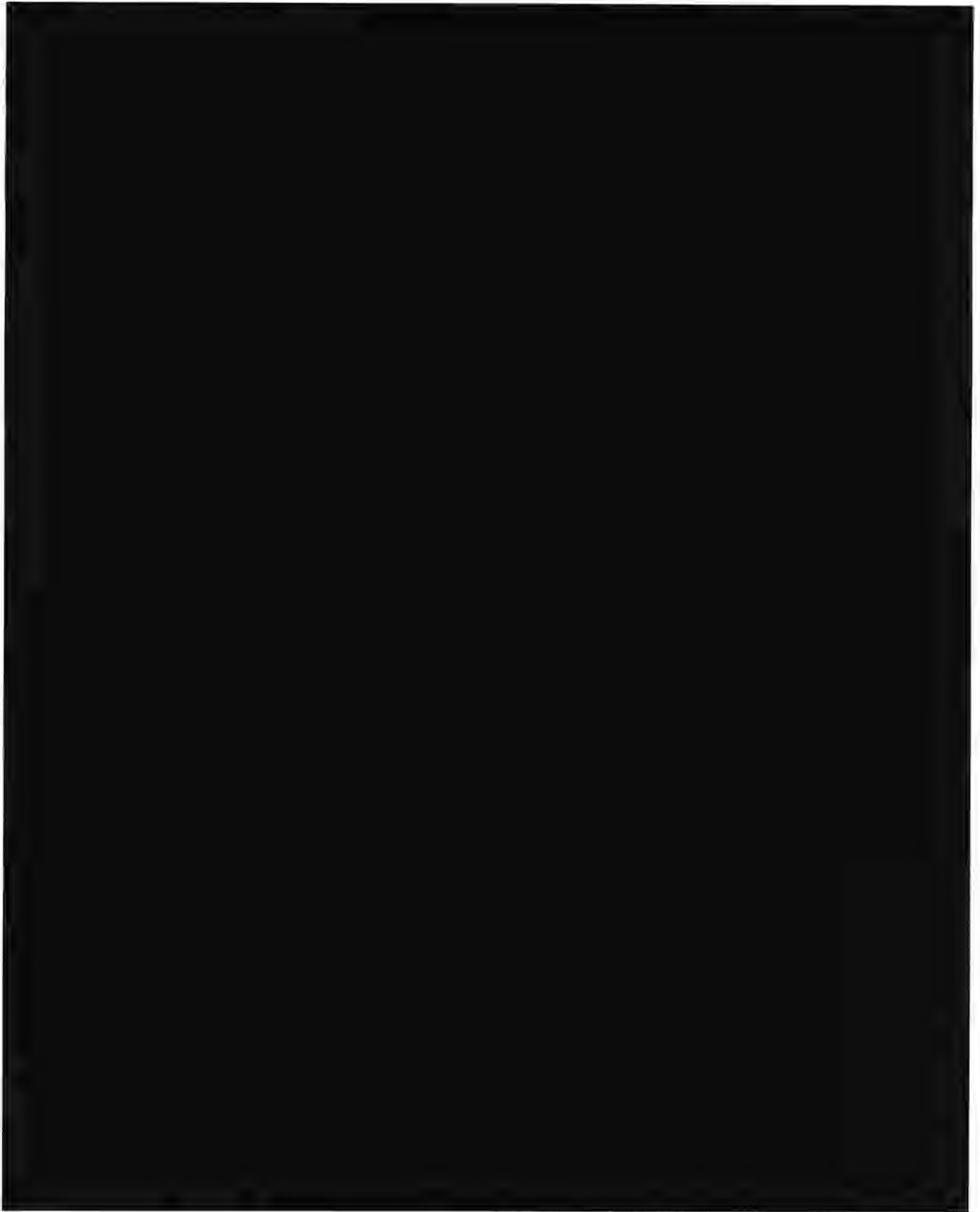
[Redacted]

The gathering of Wi-Fi data has a number of superficial privacy implications. A typical concern might be that we are logging user traffic along with sufficient data to precisely triangulate their position at a given time, along with information about what they were doing. In reality this information is of little use, since the cityblock vehicle is not in proximity to any given user for an extended period of time.

None of the data gathered by GStumbler will be presented to end users of our services in raw form.

*TODO: discuss privacy considerations with Product Counsel*







Google Inc.  
Public Policy Department  
1100 New York Avenue, NW  
Second Floor  
Washington, DC 20005



Phone 202.346.1100  
Fax 202.346.1101  
www.google.com

September 7, 2011

**CONFIDENTIAL TREATMENT REQUESTED**

*By Hand Delivery and Email*

P. Michele Ellison  
Chief, Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

Re: Google Inc., File No. EB-10-IH-4055

Dear Ms. Ellison:

Google Inc. ("Google" or the "Company") hereby responds to your August 18, 2011 letter regarding the Bureau's inquiry into Google's collection of Wi-Fi information. At all times during this matter, Google has sought to provide the Bureau with the information needed to conduct its review. We also have provided legal analysis demonstrating that no violation of Section 605 of the Communications Act occurred. Google shares the Bureau's goal of closing the inquiry promptly, and to that end continues to cooperate fully by addressing below the specific items raised in the Bureau's letter.

At the same time, Google does not agree that it somehow has failed to timely and adequately respond to any of the Bureau's prior requests. Because Google believes recent discussions with the Bureau have been productive and have resolved any prior misunderstandings, Google will not address the specific comments of the Bureau in detail in this letter.

(1) Certification of LOI Responses

The Bureau directs Google "to provide an affidavit or declaration, signed and dated by an authorized officer of the Company with personal knowledge, attesting to the accuracy and completeness of the Company's LOI responses. If such officer is relying on the personal knowledge of any other individual, rather than his or her own knowledge, provide separate affidavits or declarations of each such individual with personal

knowledge that identify clearly the responses to which each affiant or declarant with such personal knowledge is attesting.”

Company Response. Enclosed herewith are the following Declarations conforming to the Bureau’s request:

- Declaration of [REDACTED]
- Declaration of [REDACTED] Declaration addresses the Company’s December 10, 2010 Response Nos. 4(a), (h) and April 14, 2011 Supplemental Response Nos. 8 and 9 (absence of knowledge).
- Declaration of [REDACTED] Declaration addresses the Company’s December 10, 2010 Response No. 4(h) (absence of knowledge) and April 14, 2011 Supplemental Response Nos. 8 and 9 (absence of knowledge).
- Declaration of [REDACTED] Declaration addresses the Company’s April 14, 2011 Supplement Response Nos. 8 and 9.
- Declaration of [REDACTED] Declaration addresses the Company’s December 10, 2010 Response No. 4(h) (absence of knowledge) and April 14, 2011 Supplemental Response No. 9 (absence of knowledge).
- Declaration of [REDACTED] Declaration addresses the Company’s April 14, 2011 Supplemental Response Nos. 3, 8, and 11.
- Declaration of [REDACTED] Declaration addresses the Company’s December 10, 2010 Response No. 4(h) (absence of knowledge) and April 14, 2011 Supplemental Response No. 9 (absence of knowledge).
- Declaration of [REDACTED] Declaration addresses the Company’s April 14, 2011 Supplemental Response Nos. 8 and 11.
- Declaration of [REDACTED] Declaration addresses the Company’s December 10, 2010 Response Nos. 4(h) (absence of knowledge,) 9 and April 14, 2011 Supplemental Response Nos. 9 (absence of knowledge) and 11.

- Declaration of [REDACTED]  
Declaration addresses the Company's April 14, 2011 Supplemental Response Nos. 8 and 11.

As Google has previously explained, the engineer who developed the program at issue [REDACTED] is not available as a matter of law to provide a declaration. Through his counsel (whose contact information we provided on January 6, 2011), [REDACTED] has asserted his right not to testify and therefore will not execute a declaration.

(2) Certification Regarding Search

The Bureau directs Google "to produce a declaration certifying that it has conducted a comprehensive search of all materials within the Company's possession, including emails."

Company Response. The attached Declaration of [REDACTED] confirms that Google has conducted a comprehensive search for relevant materials within the Company's possession, including emails, to identify responsive documents that provide the basis for or otherwise support the Company's responses.

Google regrets the misunderstanding of Google's prior communications with the Bureau regarding the production of responsive documents. In its December 10, 2010 response, Google objected to what it perceived as an overbroad, burdensome, and non-specific production request. Google and the Bureau thereafter engaged in discussions regarding the scope of production, during which Google explained its methodology for searching for documents relevant to the response. Google assured the Bureau that it would produce responsive documents, including emails from pertinent custodians. Google promptly issued a litigation hold when investigations arose, and subsequently identified appropriate record custodians for possible production of relevant documents, including email. Google produced the documents it relied upon in its response - just as the Bureau requested. The paucity of responsive documents underscores the point that Google has made repeatedly to the Bureau in regard to the collection of payload information: there was a general lack of knowledge of the activity throughout the company and few pertinent documents.

(3) Document 11-1

The Bureau directs Google "to produce copies of all prior and subsequent versions of Document 11-1 and any other design documents for the Street View project, including the version of Document 11-1 completed on October 26, 2006, and all other responsive documents," noting that the document produced as Document 11-1 was described as having been completed on October 26, 2006, but on its face indicated that it was "Current (as of 2007-08-23)".

Company Response. Google previously submitted the most recent version of the Design Document, dated August 23, 2007 (Doc 11-1). The Design Document shows that it was completed on or about October 26, 2006, and that between October 26, 2006 and November 1, 2006, the author made additions to the technical and operational design descriptions in the document. In response to this request, Google is providing confidential Documents 11-16 through 11-20. These are the five previous versions of the Design Document, reflecting changes made between October 26, 2006 and November 1, 2006. The only change after November 1, 2006 was when the title of the Design Document was changed from "Draft" to "Current" as of August 23, 2007, as reflected in the version previously submitted as Document 11-1.

#### 4. Distribution of Document 11-1

The Bureau directs Google "to identify by name every individual to whom Document 11-1, or any prior or subsequent version thereof, was made available."

Company Response. Document 11-1 was distributed via email by [REDACTED] on October 31, 2006 to [REDACTED]

[REDACTED] It was further distributed, the same day, [REDACTED] Google does not have a reasonably accessible list of members of those listservs for 2006 as the existing list reflects only current members.

To the extent that the Bureau requires Google to disclose distribution of Document 11-1 after commencement of the Bureau's investigation, and such distribution was to attorneys, paralegals, consultants, or others engaged to provide legal advice or to assist in the representation of the Company, Google objects to the request on attorney-client privilege and work-product grounds. Document 11-1 otherwise has been made available to any requesting agency, including the Department of Justice, Federal Trade Commission, and State Attorneys General.

The Bureau previously asked Google to identify who "reviewed" the design document. The Bureau now asks the Company "to identify by name every individual to whom Document 11-1, or any prior or subsequent version thereof, was made available." Google's prior answer to the prior request was and is complete, identifying those individuals who Google confirmed *reviewed* the document. The fact that a document was shared or distributed within the Company, however, does not mean it was "reviewed" by anyone. Accordingly, Google objects to the characterization of its prior response as incomplete or pending, and it objects to the new request on the grounds of burden, relevance and feasibility of determining every person to whom the document was made available, but who did not review it.

#### (5) Translation of Foreign Language Determinations

The Bureau directs Google to "provide translations of [the] . . . final decisions of" the French Commission Nationale de l'Informatique et des Libertés ("CNIL") and the



Dutch Data Protection Agency (“DPA”), or, alternatively, to “provide an affidavit or declaration, signed and dated by an authorized officer of the Company with personal knowledge, that the Company does not have such translations.”

Company Response. Google previously informed the Bureau that it did not have official translations of the final decisions of the CNIL and the Dutch DPA. That remains true. Google’s own internal, in-country counsel has translated portions of the decisions to provide advice to the Company. Those translations are work product and attorney-client privileged, and Google objects to the request on attorney-client privilege and work-product grounds. Google offers to pay a neutral third party to translate the text of the final decisions of the CNIL and the DPA in an effort to resolve the Bureau’s request.

(6) Payload Data

The Bureau asks Google to respond to the three following questions regarding payload data; Google’s responses follow each question.

a. Whether there are any material differences in the code (i.e., “GStumbler,” “GStumblerLite,” and any other relevant code), technology, or methodology used by the Company in its Street View Wi-Fi data collection project as between the United States and other nations in which the Company collected Wi-Fi data. If so, explain why and describe such differences.

Company Response. There was no material difference in the gstumbler code used in the United States and other countries, other than the number of channels “hopped” as the vehicles drove. As is common industry knowledge, the number of channels dedicated to Wi-Fi varies from country to country (e.g., 11 in the U.S., 14 in Japan, etc.). As the Company previously stated, the vehicles channel-hopped every two seconds to maximize the identification of access points.

b. If the Company answered “yes” to Question 6.a above, would such differences result in material differences in the payload data collected in the United States and the payload data collected in other nations? In particular, in light of the evidence that intact emails, passwords, etc., were collected in other countries, is there any reason to believe that such intact payload data was not collected in the United States? If so, explain why.

Company Response. Google has no reason to believe or disbelieve that payload data collected in the United States contained “intact” user content. Google does not know and cannot speculate. Some regulatory authorities who examined payload data under their legal authorities to do so found little intelligible user content (e.g., Hong Kong, Canada) while others have stated that complete emails, for example, were present (e.g., France). Google has acknowledged publicly that data frames could contain user content, email addresses, etc. Google cannot speculate about the amount or degree of completeness of such information if present.



c. Does the Company admit that intact payload data was collected in the United States?

Company Response. Google has no factual basis to admit or deny that "intact payload" was collected in the United States.

The Letter purports to reserve the Bureau's right to request production of payload data collected in the United States. Google continues its objection thereto as stated in its December 10, 2010 Response, for all of the legal reasons stated therein.

(7) CNET Article

The Bureau references a July 25, 2011 CNET News article that stated "the Company collected the geographic locations of millions of laptops, cell phones, and other Wi-Fi enabled devices using its Street View cars, and that the locations of those devices and associated MAC identifiers were made publicly available through Google.com," and asks Google to "confirm or deny that this occurred, and [to] explain its response."

Company Response. Google provided the Bureau with the expert report of Stroz Friedberg which explained that Google collected all broadcast Wi-Fi frames within range of the Street View car, and that it parsed the MAC addresses for whatever wireless device broadcast the information. As a general principle, there is no practical way for a radio receiver to distinguish frames broadcast from a network device from those transmitted from a wireless modem. Certain assumptions can be made when the data in the header is parsed, but every wireless receiver "hears" the broadcast of the wireless device in range. The Stroz Friedberg Report documented exactly this behavior, which is what the IEEE 802.11 standard requires.

Moreover, Google expressly advised the Bureau of these facts in its April 14, 2011, and December 10, 2010, responses. In answer to Supplemental Request No. 14, Google stated:

As we previously explained, Google cannot even reliably identify the number of Wi-Fi devices from which communications were collected. Google can identify the number of basic service set identifiers (also known as "BSSIDs") which generally identify a single Wi-Fi access point that may be used by multiple stations, such as a laptop or other Wi-Fi-enabled device. The BSSID is the MAC address of the wireless access point, not the other devices, and does not indicate how many devices or networks connect through the access point itself.

Google always has explained that publicly broadcast signaling from any Wi-Fi device was received, but the purpose of the collection was to identify access points.

In regard to the Bureau's question regarding public access to location information on Google.com, the story is incorrect. A person cannot type a MAC address into a search bar and retrieve a location fix on Maps.

(8) Informational Meeting with Company Engineer

The Bureau asks Google to "provide access to an engineer, employed by the Company, with personal knowledge of the Company's Street View project, for the purposes of an in-person informational meeting to discuss technical issues."

Company Response. As Google has previously explained, and as noted above, the engineer who developed the gstumbler code and who was responsible for its deployment is legally unavailable to answer the Bureau's question. Because no one else has direct personal knowledge about the payload collection or configuration of the equipment and code written by the engineer, Google appreciates the Bureau's willingness to substitute an engineer from Stroz Freidberg to respond to the Bureau's technical questions. Per the Bureau's request, we expect that interview will take place September 9th.

In addition, Google and the Bureau have agreed to additional interviews with three other Google engineers the Bureau has identified [REDACTED], the timing of which we are discussing with your staff.

Request for Confidential Treatment

The Bureau requests that Google reexamine its requests for confidential treatment and provide amended requests, "along with copies of responsive documents with appropriate redactions." Pursuant to this request, enclosed are the following documents:

- (1) Amended Request for Confidential Treatment of Responses to Original LOI (filed December 10, 2010), Supplement to Responses to LOI (filed December 14, 2010), and Supplemental LOI (filed April 14, 2011)
- (2) Revised Redacted Responses to Original LOI (filed December 10, 2010)
- (3) Revised Redacted Responses to Supplemental LOI (filed April 14, 2011)

Google has no revisions to its Redacted Supplement to Responses to Original LOI (filed December 14, 2010), Second Supplement to Responses to Original LOI (filed December 20, 2010), or Redacted Further Response to Supplemental LOI (filed April 28, 2011).

Google has made a good faith effort to identify materials that it has made public since its prior submissions. To be clear, Google does not consider the findings of foreign

regulators, which Google may dispute, to result in a loss of confidentiality for the materials submitted to the Bureau.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'R. S. Whitt', written in a cursive style.

Richard S. Whitt  
Director/Managing Counsel,  
Telecom and Media Policy

Enclosures

cc: Theresa Cavanaugh, Acting Chief, Investigations and Hearings Division,  
Enforcement Bureau (by email)  
[REDACTED] Investigations and Hearings Division, Enforcement Bureau  
(by email)



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

September 7, 2011

*By Hand Delivery*

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of the enclosed letter from Google ("Letter") responding to the August 18, 2011, letter from P. Michele Ellison, Chief, Enforcement Bureau, Federal Communications Commission in the above-referenced matter.

As shown below, some or all of Google's responses to each of the eight items in the Bureau letter contain information that falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential,"<sup>1</sup> and/or Exemption 7(C), which provides a statutory basis for withholding from public inspection information compiled for law enforcement purposes and that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."<sup>2</sup> We enclose herewith both a complete, unredacted copy of Google's Letter, to be treated as confidential, and a separate copy of the Letter marking specific portions thereof as REDACTED.

Response to Item 1. The redacted portions of Google's response to Item 1, including the documents submitted therewith, contain detailed, specific information regarding Google's private business and internal operations, including the identity of Google employees. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2),

---

<sup>1</sup> 5 U.S.C. § 552(b)(4). See also 47 C.F.R. 0.457(d) (records not routinely available for public inspection include "trade secrets and commercial or financial information obtained from any person and privileged or confidential" under 5 U.S.C. § 552(b)(4) and 18 U.S.C. § 1905).

<sup>2</sup> 5 U.S.C. § 552(b)(7)(C). See also 47 C.F.R. 0.457(g)(3).

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 2

Google does not routinely disclose such material to the public or to third parties, has not publicly disclosed the employees' identities, and has established procedures to protect such commercially sensitive and personal information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google employees "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Response to Item 2. The redacted portions of Google's response to Item 2, including the document referenced therein, contain detailed, specific information regarding Google's private business and internal operations, including the identity of a Google employee. This information "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties and has established procedures to protect such commercially sensitive and personal information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google's business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google's employee "could reasonably be expected to constitute an unwarranted invasion of personal privacy," *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which "protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person's cooperation in the investigation or the nature of the information disclosed by that individual." *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985). Google's response to Item 2 also contains information about confidential discussions between Google and the Bureau regarding this matter.

Response to Item 3. The redacted portions of Google's response to Item 3, including Documents 11-16, 11-17, 11-18, 11-19, and 11-20 submitted therewith, contain highly confidential and contain competitively sensitive information that "would customarily be guarded from competitors." See 47 C.F.R. § 0.457(d)(2). The Documents are gstumbler project design documents and are proprietary to Google. They identify their author as a Google employee, contain references to other Google personnel, and reflect their author's subjective thoughts, analysis, and interpretation of how to carry out Wi-Fi data collection, which include the project's Objectives and Caveats (including security considerations and privacy considerations). Further, they contain trade secrets, including computer code and detailed information about and insight into Google's proprietary internal business processes (design, code, logging, testing, monitoring, documentation, work flow, and launch plans; patents; and document creation and review), all of which is proprietary to Google. Google does not routinely disclose such material to the public or to third parties, has established procedures to protect such commercially sensitive and personal



information internally, and has not publicly disclosed these documents or their contents. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the documents and the information they contain relate to business and operations of Google. See 47 C.F.R. § 0.459(a)(4). These documents also contain personally identifying information about Google employees that “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which “protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person’s cooperation in the investigation or the nature of the information disclosed by that individual.” *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Response to Item 4. The redacted portions of Google’s response to Item 4 contain detailed, specific information regarding Google’s private business and internal operations, including the identity of Google employees. This information “would customarily be guarded from competitors.” See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties and has established procedures to protect such commercially sensitive and personal information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google’s business and operations. See 47 C.F.R. § 0.459(a)(4). Disclosure of the identity of Google employees “could reasonably be expected to constitute an unwarranted invasion of personal privacy,” *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which “protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person’s cooperation in the investigation or the nature of the information disclosed by that individual.” *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985). Google’s response to Item 4 also contains information about confidential discussions between Google and the Bureau regarding this matter.

Response to Item 5. The redacted portions of Google’s response to Item 5 contain detailed, specific information regarding Google’s private business and internal operations and decisions concerning the highly sensitive subject of the Street View Wi-Fi data collection, including information about privileged discussions. This information “would customarily be guarded from competitors.” See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google’s business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Item 6. The redacted portions of Google’s response to Item 6 contain detailed, specific information regarding Google’s private business and internal operations and decisions, including proprietary computer code, technology, and methodology concerning the highly sensitive subject of the Street View Wi-Fi data collection. This information “would

**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment – File No. EB-10-IH-4055

September 7, 2011

Page 4

customarily be guarded from competitors.” See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such material to the public or to third parties, and has established procedures to protect such commercially sensitive information internally. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the redacted material relates to Google’s business and operations. See 47 C.F.R. § 0.459(a)(4).

Response to Item 7. The redacted portions of Google’s response to Item 7 conform to redactions in Google’s prior submissions.

Response to Item 8. The redacted portions of Google’s response to Item 8 contain detailed, specific information regarding the identity of Google employees and experts. This information “would customarily be guarded from competitors.” See 47 C.F.R. § 0.457(d)(2). Google does not routinely disclose such information to the public or to third parties, has not publicly disclosed the employees’ identities, and has established procedures to protect such personal information internally. Disclosure of the identity of these individuals “could reasonably be expected to constitute an unwarranted invasion of personal privacy,” *DOJ v. Reporters Comm. For Freedom of the Press*, 489 U.S. 749, 756 (1989), contrary to the purpose of FOIA Exemption 7(C), 5 U.S.C. § 552(b)(7)(C), which “protects the disclosure of the identity of individuals where such disclosure would be likely to cause harassment or embarrassment because of the person’s cooperation in the investigation or the nature of the information disclosed by that individual.” *Cuccaro v. Secretary of Labor*, 770 F.2d 355, 359 (3d Cir. 1985).

Consistent with 47 C.F.R. § 0.459(d)(1), Google requests notification by the Commission if release of the redacted material in the Letter is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
Joseph A. Bissonnette  
*Counsel to Google Inc.*

Enclosures

cc: Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau (by email)  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau (by email)





**DECLARATION OF [REDACTED]**

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]  
[REDACTED]

2. [REDACTED]  
[REDACTED]

[REDACTED] I understood that the purpose of the equipment was to identify Wi-Fi access points as the cars drove along, but I was not responsible for the Wi-Fi project or its functionality. From the Street View engineering perspective, our goal was to ensure the Wi-Fi equipment did not interfere with image collection by Street View cars.

3. I did not know that the Wi-Fi equipment installed onboard Street View vehicles could collect payload data, or that the equipment had been programmed to collect payload data from open Wi-Fi networks. I am aware that the engineer responsible who wrote the gstumbler software for use on the Street View cars, [REDACTED] prepared a design document for the project, but I do not recall reading it. Wi-Fi data collection was not within my purview. It was not until May 2010 that I first realized that payload data from open Wi-Fi networks had been collected by Street View vehicles.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 30, 2011.

[REDACTED]



**DECLARATION OF [REDACTED]**

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]

[REDACTED] Street View at the time it was proposed to use the vehicles as a platform to collect Wi-Fi access point locations for use in location-based services like Maps.

2. [REDACTED] I was aware that Google had outfitted Street View vehicles with devices that would allow them to identify Wi-Fi access points the cars drove past.

3. I was not aware at that time, however, that the Wi-Fi equipment onboard Street View vehicles could receive payload data as well, or that the equipment had been programmed to collect payload data from open Wi-Fi networks. I only learned in May 2010 that payload data from open Wi-Fi networks had actually been collected by Street View vehicles.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 30, 2011.

[REDACTED]



**DECLARATION OF [REDACTED]**

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

i. [REDACTED]  
[REDACTED]  
[REDACTED]

2. [REDACTED] I recall reviewing the gstumbler source code, which was written by [REDACTED]. In accordance with standard Google procedures, my review was limited to checking the code for proper syntax and de-bugging before the code was checked it into Google's source code repository. It was not my responsibility to review the functionality of the gstumbler code, and I did not notice that one of the features of gstumbler was the collection of unencrypted Wi-Fi communications. I have no recollection of reviewing the Wi-Fi Project design document that I understand [REDACTED] drafted and circulated, and it was not part of my duties to do so.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 30, 2011.

[REDACTED]



**DECLARATION OF [REDACTED]**

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]

[REDACTED]

2. [REDACTED]

[REDACTED] a separate team was working on collecting public Wi-Fi access point information through Street View vehicles for the same reason. The Street View project was also beginning around this time and Street View vehicles were seen as a platform that could be used for collecting these public signals. Equipment was installed on the vehicles to do just that.

3. I did not know that the Wi-Fi equipment placed onboard Street View vehicles received payload data, or that the equipment had been programmed to collect payload data from open Wi-Fi networks. I am aware that there was a design document prepared for the Wi-Fi collection, but I do not recall reading it. I did not ask that payload information be collected and it served no purpose for my projects. I am not aware of anyone else asking for payload information to be collected, and I only learned that payload data actually had been collected when various news outlets reported in May 2010 that the Street View vehicles were collecting Wi-Fi communications sent over open networks.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 31, 2011.

[REDACTED]





**DECLARATION OF [REDACTED]**

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]

[REDACTED] on the Street View vehicles.

2. In 2007, a configuration file related to the code that runs in the Street View vehicles was updated. The update concerned new Wi-Fi equipment that had been added to the vehicles. I pushed the revised configuration file to the Street View vehicles that were in the field. I did not review the configuration file, which I understand was written by [REDACTED] as doing so was not part of my job for Wi-Fi software. I only became aware that payload data had been collected when various news outlets reported that the Street View vehicles were collecting Wi-Fi communications sent over unencrypted networks in May 2010.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 31, 2011.

[REDACTED]



**DECLARATION OF [REDACTED]**

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]

2. [REDACTED]

[REDACTED]

[REDACTED]

3. The program simply relied on the presence of standard 802.11 fields in the frame headers, including MAC address, signal strength, data rate, and time stamp of a given Wi-Fi access point. Those were the only data necessary for my project and I did not use or review any other data collected by the Street View vehicles. I only became aware that payload data had been collected when various news outlets reported in May 2010 that the Street View vehicles were collecting Wi-Fi communications sent over open networks.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 31, 2011,

[REDACTED]



**DECLARATION OF** [REDACTED]

I, [REDACTED], hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]  
[REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

2. I understood that the purpose of the Wi-Fi equipment was to identify Wi-Fi access points as cars drove along for use in location-based services. The Street View team was not responsible for the functionality of the Wi-Fi equipment.

3. I was not aware that the Wi-Fi equipment onboard Street View vehicles could receive payload data or that the equipment had been programmed to collect payload data from open Wi-Fi networks. I only learned in May 2010 that payload data from open Wi-Fi networks had been collected by Street View vehicles. As a result, it was my job to implement the Company's direction to discontinue driving Street View cars around the world and to ensure the Wi-Fi collection equipment was removed from the vehicles before driving recommenced.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 30, 2011.

[REDACTED]



**DECLARATION OF [REDACTED]**

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]  
[REDACTED]

2. When Wi-Fi equipment was added to Street View vehicles, [REDACTED] the technical details that allowed the logging equipment designed by [REDACTED] to read the GPS data that Street View vehicles were already logging.

3. [REDACTED] to ensure hardware and software interoperability with the Street View vehicles' existing hardware and software, which was used to capture images and access GPS data. Testing revealed that the amount of Wi-Fi data being collected was miniscule relative to the size of the images and GPS data that the Street View cars already were collecting, and would not pose any technical problems. I did work with [REDACTED] to resolve a minor bug that was causing the program to shutdown at one point. But that bug was unrelated to any payload collection and in the course of resolving the bug I never learned that any payload was being collected.

4. I recall receiving the design document prepared by [REDACTED], but I do not recall any reference to payload collection. I was not aware at that time that the Wi-Fi equipment onboard Street View vehicles could receive payload data. I only became aware that payload data



had in fact been collected when various news outlets reported in May 2010 that the Street View vehicles were collecting Wi-Fi communications sent over unencrypted networks.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 31, 2011.





**DECLARATION OF** [REDACTED]

I, [REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]  
[REDACTED]

2. Google allows its engineers to dedicate up to 20 percent of their time to work on projects of interest to them that are not within the normal scope of their job. This is known as the "20% Program."

3. As part of the 20% Program, a Google engineer named [REDACTED] undertook in mid-2007 to outfit Google's Street View vehicles with devices that would allow them to identify Wi-Fi access points the cars drove past. This data could then be used in future location-based services.

4. Although Wi-Fi collection had nothing to do with the Street View project, Street View vehicles were an ideal platform for this collection. [REDACTED] drafted a design document (essentially a project summary and proposal) for the Wi-Fi project and wrote the necessary code to store data publicly broadcast from access points. I have no recollection of reading the design document.

5. I did not request that [REDACTED] program the Street View equipment to collect payload data, nor did I think about the collection of that data as possibility because the purpose was to correlate public access point information with GPS signals to assist in determining location. I only became aware that payload data had in fact been collected when various news outlets reported that the Street View vehicles were collecting Wi-Fi communications sent over unencrypted networks, and I frankly thought the reports were wrong.

6. To my knowledge the payload data collected by the Street View vehicles has never been included in any product or service, and no product manager requested that the payload be collected for any product or service. [REDACTED] I would expect that if anyone had wanted to use payload in a product or service, they would have necessarily asked me. No one ever did.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 30, 2011.

[REDACTED]



DECLARATION OF [REDACTED]

[REDACTED] hereby submit this declaration in connection with Google Inc.'s ("Google") responses to the Federal Communications Commission's requests for information in File No. EB-10-IH-4055. I declare as follows:

1. [REDACTED]

2. I have personal knowledge of the representations that the Company made in its Responses to P. Michelle Ellison, Chief of the Federal Communications Commission Enforcement Bureau, including the representations made in the Company's September 7, 2011, letter to the Bureau, and hereby verify the truth, accuracy and completeness of the same.

3. As described in Google's September 7, 2011 letter, the Company has conducted a comprehensive search for relevant materials in its possession, including emails, in response to the Bureau's requests.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on September 6, 2011.

[REDACTED]



# CNIL

The Chairman

The Manager  
GOOGLE Inc.  
1600 Amphitheatre Parkway  
Mountain View, CA 94043  
UNITED STATES OF AMERICA

## LETTER DELIVERED AGAINST SIGNATURE

*References to quote in all correspondence:*  
CTX-2010-050

Paris, 18 March 2011

Dear Sir,

Please find attached decision no. 2011-035, adopted by the restricted committee of the Commission Nationale de l'Informatique et des Libertés, imposing a financial penalty of 100,000 Euros on your company and ordering publication of this decision on the Commission's Internet site and the Légifrance Internet site.

As far as the procedure relative to recovering the financial penalty is concerned, I wish to inform you that, during the course of the next few months, you will receive a writ of execution issued by the treasurer of the Consulate General of France.

I wish to make it clear that you have a period of two months starting on the date of notification of the decision within which to lodge an appeal against it before the Council of State should you so wish.

In addition, I wish to inform you that, in response to your request in this matter, the Commission considers that you may now destroy the content data ("payload data") collected by the vehicles known as "Google cars" on French territory.

Should you require any further information, please contact Ms. Elise WOLTON, head of the sanctions management department (33 (0)1 53 73 25 44/25 37).

Yours faithfully,

Enclosure: decision no. 2011-035

Alex TÜRK

For the Chairman  
The General Secretary  
Yann PADOVA



**Decision no. 2011-035 of the restricted committee imposing a financial penalty  
on the company GOOGLE Inc.**

The Commission Nationale de l'Informatique et des Libertés, meeting in restricted committee, chaired by Mr. Alex TÜRK;

Also present: Mr. Emmanuel de GIVRY, deputy vice-chairman, Ms. Isabelle FALQUE-PIERROTIN, vice-chairwoman, Ms. Claire DAVAL, Mr. Sébastien HUYGHE and Mr. Jean-Marie COTTERET, members;

In view of the Council of Europe's Agreement no. 108 of 28 January 1981 relative to the protection of persons with regard to automatic processing of data of a personal nature.

In view of law no. 78-17 of 6 January 1978 relative to data processing, data files and individual liberties, amended by law no. 2004-801 of 6 August 2004 and, in particular, its 1<sup>st</sup> article.

In view of decree no. 2005-1309 of 20 October 2005 issued for application of law no. 78-17 of 6 January 1978 relative to data processing, data files and individual liberties, amended by decree no. 2007-451 of 25 March 2007.

In view of deliberation no. 2006-147 of 23 May 2006 defining the rules of procedure of the Commission National de l'Informatique et des Libertés.

In view of deliberation no. 2010-216, adopted in emergency session by the Commission's executive committee on 26 May 2010, addressing formal notice to the company GOOGLE Inc.

In view of decisions no. 2009-231C of 4 December 2009 and no. 2010-140C of 17 May 2010 made by the Commission's chairman to proceed with an on-site inspection of the compliance with law no. 78-17 of 6 January 1978 amended of the "*Street View*" system implemented by the company GOOGLE Inc., represented in France by the company GOOGLE France.

In view of the report submitted by Mr. Philippe GOSSELIN, commissioner recorder, to the company GOOGLE Inc. by letter dated 28 October 2010 and received on 1 November 2010, a copy of which was also sent to the company GOOGLE France by letter dated 28 October 2010 and received on 29 October 2010.

In view of the remarks in response to the latter, dated 28 December 2010.

In view of the other elements of the case.

Having heard the following at its meeting held on 6 January 2011:

- Mr. Philippe GOSSELIN, commissioner, on his report.
- Mr. Peter FLEISCHER, the company GOOGLE Inc.'s personal-data protection manager, Mr. Olivier ESPER, corporate relations manager, Mr. Benjamin AMAUDRIC DU CHAFFAUT, legal manager, Mr. Laurent GRAVE-RAULIN, from the company GOOGLE France and Ms. Ariane MOLE, lawyer, their legal advisor.

Ms. Elisabeth ROLIN, Government commissioner, not having heard the remarks made.

The representatives of the company summoned having taken the floor last.

## I. REMINDER OF THE FACTS

### 1. Presentation of the company GOOGLE Inc. and the services proposed

The principal activity of the company GOOGLE Inc. (hereafter, "the company") is the search for information on the Internet, development of services on the Internet and on-line advertising.

In particular, it has developed geographic search tools based on satellite or aerial photographs and on photographs taken in public places and on public highways. It has added additional functions to these cartographic tools, such as geolocalisation, which makes it possible to determine the position of a user of the service.

The company initially launched the on-line service "*Google Maps*" (in 2004), which makes it possible to view a geographic area on-line from a country scale right down to a street scale. The maps proposed come from both conventional mapping data (borders, streets, motorways, etc.) and from very accurate satellite or aerial images. This service was extended to France in April 2006.

In 2007, it added the "*Google Street View*" service to the "*Google Maps*" service (hereafter, *Street View*), thus offering Internet users a panoramic view of streets, 360° horizontally and 290° vertically. The images displayed are created from photographs taken by the company GOOGLE Inc. throughout the world using vehicles equipped with digital cameras. The photographs are placed end-to-end to create the image. These vehicles are usually referred to by the term "*Google Cars*."

The company GOOGLE France announced the extension of the *Street View* service to French territory in June 2008. It declared to the Commission Nationale de l'Informatique et des Libertés (hereafter "CNIL" or "the Commission") on 1 July 2008 that the purpose of the processing operation was "*to make available the Google Street View Internet service*" on behalf of the company GOOGLE Inc. (declaration no. 1303459).

In February 2009, the company GOOGLE Inc. added the "*Google Latitude*" geolocalisation service to the mobile function of "*Google Maps*" ("*Google Maps Mobile*"). This new service allows the user, on condition that he/she has both a Google account and the *Latitude* application installed on his/her advanced telephone ("*smartphone*"), to display his/her position and thus indicate to friends where he/she is in real time. Conversely, it also allows geolocalisation of friends or family on a map or list if they have the same equipment.

Operation of all the geolocalisation services via the WiFi networks or GSM networks that the company proposes (including *Google Maps*, *Google Street View* and, consequently, *Latitude*) depends on the constitution and updating of a common database, called the "*GLS base*," standing for "*Google Location Server*."

The company created this database in successive stages. An essential stage in its initial development consisted of a massive collection of radio signals (GSM and WiFi) associated with GPS positions by the "*Google cars*" in the context of the *Street View* programme.

Today, enrichment and updating of the base proceeds essentially via the collection of data captured and transmitted in a recurrent manner by the users connected to this service via their mobile telephones and terminals, i.e. the MAC addresses<sup>1</sup> and SSID identifiers<sup>2</sup> of the WiFi access points<sup>3</sup> located in their proximity.

Recording of data received from these terminals makes it possible to update the information contained in the GLS base continuously. It is this continuous collection of data, achieved by means of the users' mobile terminals, that thus allows the company to optimise the geolocalisation services via the networks it proposes to its customers.

## **2. Exchanges between CNIL and GOOGLE France concerning the *Latitude* service (February 2009 - April 2010)**

In February 2009, GOOGLE Inc. announced the launch of *Latitude* in 27 countries, including France.

Following exchanges between CNIL and the company GOOGLE France concerning the operation of *Latitude*, particularly during a meeting on CNIL's premises on 6 February 2009 and other subsequent exchanges by letter, CNIL's chairman addressed a letter to the company, dated 14 May 2009, indicating that it considered this service to involve the processing of data of a personal nature, which is governed by the law 6 January 1978 amended and that, in this regard, in compliance with article 22 of the said law, the processing operations had to be the subject of a declaration addressed to its services.

The company contested this analysis in a reply by letter, dated 3 August 2009, considering that these processing operations were not subject to French law since the data in question was not, in its opinion, collected using processing resources located on French territory.

Consequently, it refused to declare *Latitude* to CNIL.

By letter, dated 29 October 2009, received by the Commission on 21 December 2009, the company GOOGLE France informed CNIL of its wish to appoint a personal-data protection correspondent. The appointment came into effect on 29 January 2010.

CNIL's services again questioned GOOGLE France about the data-collection procedures used in the context of the *Latitude* service in an e-mail dated 8 January 2010.

In its reply by e-mail, dated 8 February 2010, the company indicated that the geolocalisation database on which its service depends (GLS base) was constituted in three successive stages, i.e.:

- Initially with information contained in the queries from users of Google Maps Mobile using the "cell ID" [GSM aerial identifier] and the centre of the map displayed, based on the hypothesis according to which, statistically, the terminal is located in the surrounding area.
- Secondly, GPS and WiFi information was added when it happened to be included in the Google Maps Mobile users' queries.
- Finally, the *Street View* cars were used to feed the database using GPS and radio signals.

---

<sup>1</sup> MAC (Media Access Control) address: unique number identifying a network card.

<sup>2</sup> SSID (Service Set Identifier): name identifying a wireless network.

<sup>3</sup> WiFi (abbreviation for Wireless Fidelity): technology enabling the wireless connection of several computer devices (computer, router, Internet decoder, etc.) in a computer network.

In view of this reply, CNIL's chairman informed the company by letter, dated 20 April 2010, that the Commission maintained its interpretation, according to which *Latitude* requires the deployment of processing resources on French territory, such as *Street View* and that consequently, this service should be the subject of prior formalities in France.

### 3. Initial inspections conducted by CNIL

On 11 December 2009, CNIL's services proceeded with an on-site inspection of the company GOOGLE France, representing the company GOOGLE Inc., in order to check compliance of the *Street View* service with the provisions of the law of 6 January 1978 amended.

During this inspection, the company presented the technical resources implemented to record the photographs taken by the "*Google cars*." The inspectors noted that these vehicles were equipped with several digital cameras and a device recording GPS data.

The company was asked to indicate to CNIL, within five days, if the vehicles used collected technical information other than GPS data and photographs. The outcome of the subsequent exchanges with the company is that CNIL did not obtain details on this point within the specified deadlines.

As agreed with the company at the time of the on-site inspection on 11 December 2009, the Commission proceeded with a new inspection mission with the company on 18 January 2010 in order to examine a "*Google car*" vehicle in working order.

The inspection delegation noted the presence of several data-collection devices on the vehicle's roof and a WiFi key, which is used to capture and record WiFi signals, in the vehicle's boot. It was nevertheless unable to determine the exact nature of the data recorded by the device since the vehicle presented to the delegation was not equipped with a hard disk for data-collection.

The inspection delegation therefore reiterated the request previously made concerning the nature of the data collected and asked for the purpose of WiFi-signal collection to be specified. The company undertook to reply to the Commission within five working days on these two points and various other questions remaining pending; this undertaking was noted in the inspection report.

By letter, dated 28 January 2010 and forwarded by the company GOOGLE France, GOOGLE Inc. indicated to the Commission that:

- The vehicles are equipped with GPS devices to track their position and thus allow this information to be associated with the images collected.
- In addition, they contain laser equipment to assist in measuring distances between objects and a device enabling connection to wireless networks (WiFi) and their identification.
- The information concerning these wireless networks can be used by users who have activated the geolocalisation services available with certain products (e.g. "*Google Maps*") to facilitate the supply of local information relevant to him/her.

By letter, dated 9 February 2010, CNIL questioned the company in a more precise manner about the data collected *via* the device allowing the vehicles to connect to wireless networks (WiFi) and identify them.



The company replied to this question on 25 February 2010, stating that this collection only concerned the WiFi network identifiers (Service Set Identifiers (SSID)) and MAC addresses of the WiFi routers, collected in the context of the geolocalisation services.

On 27 April 2010, the company GOOGLE Inc. published a communiqué on its blog intended to answer the questions relayed by the international press concerning the data recorded by its "Google cars," indicating that *"the networks [WiFi] send information to the other computers in the network, called communication content or payload data but Google neither collects nor stores such data"*<sup>4</sup>. On the same day, GOOGLE France confirmed to CNIL by e-mail that collection by its vehicles of WiFi data intended for its localisation services in no way concerned communication content data.

However, on 14 May 2010, the company published a press release admitting the collection of content data. This collection, qualified as involuntary, would be the consequence of an error in programming the collection software's source code (i.e. all the code lines that ensure operation of the software), committed in 2006. Installation of this software in the "Google cars" would have allowed the recording of *"fragments of communication-content data"* as from the date of entry into service of the vehicles in 2007.

Following these disclosures and in view of the seriousness of the facts revealed and the need to act quickly, the Commission proceeded with a new on-site inspection of GOOGLE France, representing GOOGLE Inc., on 19 May 2010. The aim of this inspection was to note the nature of the data effectively collected by the "Google cars" on French territory and the measures taken by the company following these disclosures.

Apart from the WiFi key installed in the boot and the collection devices on the roof, the vehicle examined during this inspection effectively contained a collection hard disk recording the data captured, unlike the vehicle examined during the inspection of 18 January 2010. In addition, the company indicated that these vehicles would no longer proceed with the collection of data relative to WiFi data and that it was awaiting the consent of the national data-protection authorities to proceed with the deletion of the data and particularly from CNIL concerning the data collected in France.

At the end of the inspection, the delegation asked for CNIL to be provided with technical information concerning the collection of WiFi data along with copies on an IT medium and, in particular, a complete copy of all the content data originating from WiFi terminals in France and this, within a period of 3 working days.

The requests for information mentioned in the report are as follows:

- What are the criteria that made it possible to isolate the data collected relative to content originating from WiFi terminals (*"payload data"*)?
- Was content data from secure WiFi terminals collected? If yes, under what conditions is it processed?

---

<sup>4</sup> "Networks also send information to other computers that are using the network, called payload data but Google does not collect or store payload data."

The requests for computer copies were the following:

- The last hard disk from a collection operation executed by a Street View vehicle in France sent to the United States.
- The code of the computer program used in the Street View vehicles up to 14 May 2010, identifying the part of the code that resulted in the collection of data relative to content from WiFi terminals ("*payload data*").
- The data relative to content from WiFi terminals in France, isolated by GOOGLE Inc.
- The new code now used by the company in the context of collection operations conducted by the *Street View* vehicles (transmission deadline: as soon as the code is validated).
- The audit conducted at the request of GOOGLE Inc., as announced in its press release of 14 May 2010.

By e-mail, dated 21 May 2010, the company GOOGLE France informed the Commission that the previously mentioned requests had been forwarded to the company GOOGLE Inc. In addition, it indicated that it would be "*very probably impossible to comply with the required deadline*" for the computer copies requested because of the location of these elements in the United States and similar requests from various European data-protection authorities.

After the inspection, the inspectors also asked for CNIL to be informed of any resumption of collection operations by the *Street View* vehicles in France in order to be present at the resumption and obtain copies of the data recorded.

#### **4. Formal notice addressed to the company GOOGLE Inc. by CNIL on 26 May 2010 and the company's replies**

Noting the failure to submit the computer copies indicated in the inspection report of 19 May 2010 within the specified deadlines, the Commission's executive committee addressed formal notice to the company on 26 May 2010 on the grounds of urgency (decision no. 2010-216 of 26 May 2010). Google Inc. was informed of this decision by registered letter, dated 27 May 2010, with acknowledgement of receipt on 7 June 2010. A letter informing the company Google France, representing the company Google Inc., was also delivered to the addressee in person on 28 May 2010.

This formal notice was adopted on the grounds of urgency in view of the seriousness of the acts, the significant number of people involved and the nature of the data processed. In particular, the Commission's executive committee noted in this regard that the data collected by the company, such as that from WiFi terminals, was likely to contain information on the Internet sites consulted by the people in question, on the content of messages exchanged and on the identifiers and passwords enabling connection to certain sites and this, for several years, and that this collection was of a nature to constitute a serious violation of the rights and liberties protected by article 1 of the law of 6 January 1978 amended, particularly privacy, secrecy of correspondence and freedom of speech.

This decision of the Commission's executive committee thus gave formal notice to the company to execute the following within a period of seven days starting on the date of notice:

- Proceed with the formalities specified in Chapter IV of the above-mentioned law of 6 January 1978 for "*Google Latitude*" processing.
- Cease all collection of data without the knowledge of the people concerned in the context of "*Google Street View*" processing, particularly concerning WiFi network identifiers (SSID), MAC addresses of WiFi routers and connection data from WiFi terminals.

- Ensure that data of a personal nature is no longer collected in a dishonest or unlawful manner in the context of "Google Street View" processing.
- Communicate to the Commission the information and copies requested during the on-site inspection conducted on 19 May 2010, as indicated in the report and, in particular, provide CNIL with a copy on an IT medium of all data collected in France via WiFi terminals in the context of "Google Street View" processing.
- Prove to CNIL that all the above-mentioned requests have effectively been satisfied within the specified deadlines.

In order, in particular, to obtain communication of the computer copies indicated in the formal notice and particularly the data recorded during access to WiFi networks on French territory and the source code that enabled collection, the Commission proceeded with a new on-site inspection of the company GOOGLE France on 4 June 2010 following a prior agreement concluded with it.

After the inspection, the company gave the delegation a copy of the hard disk containing all the information collected by a *Google car* in the area surrounding the town of MILLAU in April and May 2010.

It also submitted a second disk containing a copy of the connection data recorded on French territory, a copy of a report on an audit of the source code conducted at the request of the company GOOGLE Inc. by the STROZ FRIEDBERG office and a copy of the part of the source code that resulted in the collection of data relative to content from WiFi terminals. The company did not submit the entire source code used by the "Google cars," considering that the request made by CNIL concerned *"only the computer program that served to collect WiFi data (the program called "gStumbler") and not the entirety of the software used by the Street View vehicles."*

In a letter dated 4 June 2010, the company replied as follows to the formal notice adopted by the Commission's executive committee:

On completion of prior formalities with CNIL: the company maintains in its remarks that the data processing operations conducted in the context of the *Latitude* service do not, in its opinion, have to be declared to CNIL. However, *"despite its doubts,"* the company announced amendments to the declaration submitted to CNIL concerning the *Street View* service. These amendments consist, first of all, of adding the information on vehicle positioning, the data from the accelerometer, the vehicle's laser beam, the SSID identifiers and the MAC addresses of the WiFi routers to the "data collected" item. Secondly, the provision of geolocalisation services and the creation of geographic maps were added to the "declared purposes" item. These two additions were made by the company *"with a view to complying with the formal notice and without prejudice."*

Concerning the collection of data without the knowledge of the people concerned in the context of "Google Street View" processing: the company continues to maintain that it has ceased all collection of WiFi data using "Google cars." Cessation of this collection particularly concerns WiFi network identifiers (SSID), WiFi router MAC addresses and connection data from WiFi terminals.

Concerning dishonest or unlawful collection of data: the company indicates that it has ceased all collection of WiFi data using "Google cars"; in addition, it contests the dishonest or unlawful characterisation that would attach to this collection since it was unintentional.



Concerning the requests for information and computer copies: the company reminds, in particular, that it submitted a copy of the STROZ FRIEDBERG report to the Commission during the inspection on 4 June. It indicates that the *"copy of the last hard disk sent to the United States containing data from a collection operation conducted by a Street View vehicle in France"* and the copy of *"data relative to content from WiFi terminals in France, isolated by GOOGLE Inc."* were submitted to the Commission during the inspection on 4 June 2010.

The company adds that, during the inspection on 4 June, it submitted *"the source code of the program used in the 'Street View' vehicles serving to collect payload,"* i.e. the collection of content data, reminding that it considered the Commission's request to concern only the software that served to collect WiFi data, called *"gStumbler"* and not the entirety of the software implemented in the vehicles.

In addition, by e-mail dated 12 July 2010, the company sent CNIL a new version of the *"gStumbler"* software since, according to the company, the version supplied during the inspection on 4 June 2010 was not the right one.

Concerning the source code of the software that will be implemented on resumption of collection operations: the company indicates that it has ceased to collect data relative to WiFi terminals using *"Google cars"* and that it will give CNIL a copy of the one or more new software packages implemented, not including WiFi data-collection functions, as soon as these elements become available.

## **5. Analysis of elements submitted by the company during the inspection on 4 June 2010**

After the inspection on 4 June 2010, the company submitted computer copies to CNIL, in particular, of data recorded by GOOGLE Inc. during access to WiFi networks on French territory and the source code that enabled its collection. It also submitted the report on the audit of this source code, called the STROZ FRIEDBERG report.

### Source code of the WiFi data-collection software

Via its formal notice of 26 May 2010, CNIL enjoined the company to submit various elements indicated in the inspection report of 19 May 2010, of which *"the code of the computer program used by GOOGLE Inc. in 'Google cars' up to 14 May 2010, identifying the part of the code that resulted in the collection of data relative to content from WiFi terminals ('payload data')."*

In response to this injunction, during the above-mentioned inspection on 4 June 2010, the company submitted the source code of the computer program used in the *Street View* vehicles that enabled collection of content data to the Commission, with the reminder that it considered the Commission's request to concern only the software that served to collect WiFi data, called *"gStumbler."* In addition, by e-mail dated 12 July 2010, the company sent CNIL a new version of the *"gStumbler"* software since, according to the company, the previous version was not the right one.

Analysis of the source code submitted during the inspection showed that the company submitted only the source code relative to calculation of the GPS position of the moving *"Google car"*; in addition, analysis of the new source code elements supplied by e-mail on 14 July 2010, showed that these latter elements were limited to the launch code of the WiFi data-collection tool. These new elements did not therefore make it possible to determine the operation of the software collecting content-data from WiFi terminals any more than the source code submitted during the inspection.



However, the STROZ FRIEDBERG report, the compilers of which, for their part, had access to the whole source code, accurately analysed the software developed and implemented by the company.

Thus, this report shows that the software deployed in the data-collection vehicles, called *gSlite*, was developed by the company in 2006 in the context of the *gStumbler* project. This software includes a program for detecting and capturing wireless content data, called *Kismet*, which captures and records all WiFi data within its range (encrypted and unencrypted data, control data and management data). The *gSlite* software adds GPS data to the WiFi data captured and recorded by *Kismet* in order to locate them accurately.

In addition, it turns out that *gSlite* was developed to collect and store unencrypted content data, control data and management data by default. The default parameters of *gSlite* can be changed during use to limit the categories of data stored. The company did not change the software's parameters in this way when it was deployed in the *Google cars*, with the result that as soon as it was implemented it had the possibility to record content data.

In addition, the company did not submit to the Commission any element, even partial, of the new collection software's source code as indicated in the formal notice of 26 May 2010.

#### Concerning content data captured by the "Google Cars"

During the inspection on 4 June 2010, the company GOOGLE Inc. submitted a copy of the content data recorded in France to the Commission's delegation. The report specifies that this is *"WiFi content data ("payload"), isolated from the other data and collected for the whole of France by all the "Google cars."*

Firstly, analysis of this data, which was conducted by the Commission's services, shows that the *"Google cars"* did effectively collect content data from unsecured WiFi terminals over a large part of French territory. More than 50% of the territory was thus covered, including all urban areas and in particular the cities of Paris, Lille, Lyon, Bordeaux, Marseille, Toulouse, Caen, Rennes, Strasbourg, Clermont-Ferrand and Nice.

The data submitted to CNIL represents a volume of 16.8 GB. In this set of data, the exploitable volume amounts to approximately 1,400 Mb, i.e. 8% of the total volume of data analysed.

Among these, by conducting searches based on key words, the Commission was able to isolate 656 Mb of data relative to navigation on the Internet, showing the presence of 112 passwords for accessing Internet sites (http) and a considerable quantity of data for connecting to online dating and pornographic sites.

Proceeding by simple query by key word, the Commission also isolated 6 Mb of access data for electronic mailboxes, including 72 messaging passwords. Among the mail transfer data (smtp), CNIL was able to identify 124 electronic mail addresses concerning both senders and recipients. In general terms, the Commission was able to identify 774 distinct electronic mail addresses in the set of data submitted.

As for the analysis of content data, it was possible to determine with great accuracy the nature of the sites consulted, the passwords for accessing them and the geographic location of the user. It was also possible to achieve a certain number of reconciliations, for example:

- On 2 June 2008 at 12.46 p.m., an Internet user located, according to the GPS data, close to a precise address in the city of MARSEILLE (13007), accesses the pornographic image site <http://www.straightboysjerkoff.com>, of which he is a member. The identifier he uses on the site is recorded in cleartext as are his password and IP address on the internal network connected to his access point. The SSID identifier and MAC address of his access point are known to Google but were deleted from the information submitted to CNIL.
- On 21 October 2008 at 1.05 p.m., an Internet user located, according to the GPS data, near the Place Anne de Beaujeu in TOURS (37000), accesses the gay online dating site <http://rencontres.gayvox.com>. His IP address on the internal network connected to his access point was recorded.
- On 26 March 2009 at 3.03 p.m., an Internet user who could be located very accurately via his GPS coordinates on the D118 road (north of Carcassonne), accesses the online dating site <http://www.mes-rencontres-sexy.com>, of which he is a member. The identifier used is known to the company, as are his password and IP address on the internal network connected to his access point. Again, the SSID identifier and MAC address of his access point are known to Google but were deleted from the information submitted to CNIL. Before arriving at the site, according to the cookies intercepted, the Internet user launched the following search on the Google search engine: "free naughty encounter."
- Fragments of access to an online healthcare system close to the GPS coordinates of the Clinique Mutualise Chirurgicale, located at 3 rue Le Verrier in Saint Etienne (42100) were also intercepted. These fragments refer, in particular, to an act prescribed by a healthcare professional, who is named and the access path to the documents sought refers to a tool for managing patients in a hospital environment.
- It was also possible to consult an exchange of e-mails between a married man and woman, both seeking an extra-marital relationship. The GPS coordinates associated with this query, identified in cleartext, point to a precise address (a street number in a town in the Rhône department). The people in question are identified by their first names and e-mail addresses.

These reconciliations were made by CNIL without any particular difficulty although the SSID identifiers and MAC addresses of these users' access points (known to Google) had, on the other hand, been deleted from the information submitted.

#### Concerning SSID identifiers and MAC addresses captured by the Google cars

During the inspection of 4 June 2010, the company GOOGLE Inc. submitted a copy "of a hard disk containing all the information collected following a collection operation executed by a Street View vehicle (area surrounding the town of MILLAU, April-May 2010)" to the Commission's delegation.

Analysis of this hard disk, which corresponds to a journey on the major roads of the Languedoc-Roussillon region, revealed the presence of more than 6,000 SSID identifiers and more than 185,000 MAC addresses.

In addition, it made it possible to establish that the "Google cars" recorded not only the MAC addresses of the WiFi access points but also the MAC addresses of all the terminals collected at these access points (PCs, printers and other peripherals, *smartphones*, etc.).

## **6. The "informal opinion" request made by the company on resumption of Google car activities (15 July 2010)**

By e-mail, dated 15 July 2010, the company informed the Commission that it was planning *"the extension, or not, of contracts relative to the Google cars and their drivers."* It specified that *"on resumption of activities, the cars will no longer contain any WiFi collection equipment."* At the end of this e-mail, the company requested an *"informal opinion"* from the Commission *"on the link with the procedure in progress."*

The Commission's services replied to this request on 16 July 2010, specifying that *"in compliance with the specifications of the report drafted at the time of the inspection conducted on 19 May 2010, CNIL asks to be informed as soon as a Street View vehicle resumes collection of data in France to allow a CNIL delegation to be present during collection operations and obtain a copy of the information collected at that time for analysis purposes."*

In view of the formal notice procedure in progress, the services refrained from delivering any informal opinion concerning the resumption of *Google car* activities; incidentally, formulation of an opinion of this nature is not provided for by law.

## **7. Inspection concerning the *Latitude* service following issue of formal notice**

The Commission's services proceeded with an on-site inspection of the company GOOGLE France on 21 July 2010 to obtain details on the technical characteristics of the geolocalisation services proposed by the company, including the *Latitude* service, since their previous requests in this matter had remained without effect.

During the inspection, the company specified the scope of the amending declaration concerning the *Street View* service received by the Commission on 8 June 2010. They informed the delegation that the above-mentioned amendment *"aims to regularise the formality completed by including the WiFi data collected up till now. This amendment also aims to specify that the WiFi data collected is used in the context of the geolocalisation applications proposed by GOOGLE."*

After this inspection, the delegation submitted the copy of a questionnaire to the company, already addressed on 13 July 2010, including the following question in particular: *"Do Google's geolocalisation services (used by Latitude) require the SSID of a WiFi access point in order to recognise it? Is the MAC address not sufficient?"*

In its reply by letter, dated 3 August 2010 (subsequently completed by a letter, dated 15 September 2010), the company submitted elements of response to this questionnaire to CNIL, indicating, in particular, that the company was not using SSID data to provide the *Latitude* service at that time.

## **8. Inspection of 30 July 2010**

The Commission again proceeded with an inspection mission on 30 July 2010 to examine the operation and technical characteristics of a *"Google car"* following the formal notice of 26 May 2010. This inspection took place partially on the Commission's premises, in coordination with the company.



The delegation proceeded with an examination of the technical devices implemented in the vehicle, particularly the collection devices (cameras, aerials, gyroscope, etc.). It was informed by the company that *"the vehicle has no means of capturing WiFi signals and that no WiFi data will be collected by the vehicle."*

The vehicle's collection hard disk, which had to be submitted to the delegation after a journey in Paris, could not be submitted on account of *"the technical impossibility to read and copy this disk."* The company then proposed that the Commission keep the un-exploitable collection hard disk. The Commission accepted.

It was not until after a second inspection, conducted on 11 August 2010 and analysis of the hard disk submitted by the company, that it became clear that the data recorded effectively consisted of photographs and GPS data and no longer included any WiFi data files.

Following the inspection, the company was also asked to indicate if the identifiers of GSM aerials (*"Cell IDs"*) were recorded by its vehicles. The company replied by e-mail, dated 13 August 2010, that it did not collect such data by means of *Street View* vehicles while, at the same time, specifying that this data was collected in the context of other services, such as *Google Maps*.

## **9. Announcement of resumption of *Google car* activities by the company**

By e-mail, dated 18 August 2010, the company informed CNIL that, on the following day, it would publicly announce the resumption of presence of the *Street View* service's cars on the roads of France.

The following day, the Commission addressed a registered letter to GOOGLE Inc., dated 19 August 2010, reminding it that *"as things stand, GOOGLE Inc. has not yet supplied all the answers or elements requested in the formal notice of 26 May 2010 and during the course of subsequent inspections."* The letter adds that *"the resumption of "Google car" activities and their collection operations would place [the] company in a vulnerable legal situation insofar as the restricted committee has not yet delivered its decision [on appropriate action pursuant to the formal notice]."*

The resumption of *Google car* activities was effectively announced publicly on 19 August 2010, despite the fact that proceedings were already in progress following adoption of the formal notice on 26 May 2010 and the pursuit of inspections.

## **10. Inspection conducted following resumption of *Google car* activities**

Following this announcement, the Commission proceeded with an on-site inspection of the company on 25 August 2010 to examine the operation of a *"Google car."*

During the inspection, the delegation was informed that 22 *"Google car"* vehicles had been sent out on the road again in France, of which one in Île de France. Having noted the absence of WiFi aerials and *gSlide* software on the list of software installed in the vehicle, it proceeded with a journey of approximately one hour in the vehicle.

After the journey, the delegation proceeded with analysis of the on-board hard disk and noted that the data recorded consisted of photographs and GPS data and did not include WiFi data files.

## II. PROCEDURE

On the basis of these exchanges and the findings noted during the on-site inspection missions conducted after the issue of formal notice, the Commission initiated proceedings against the company GOOGLE Inc. pursuant to paragraph 1, section 1 of article 45 of the law of 6 January 1978 amended, which stipulates:

*"I - The Commission Nationale de Informatique et des Libertés may (...) issue notice to the data controller to put an end to the breach observed within a time limit that it determines. If the data controller does not comply with the formal notice addressed to him/her, the commission may impose the following penalties after an adversary procedure:*

*1 - A financial penalty, within the conditions provided for in article 47, except in cases where the processing is carried out by the State, (...)."*

The report compiled by Mr. Philippe GOSSELIN, CNIL member and recorder, proposing that CNIL's restricted committee impose a financial penalty of €150,000 on the company GOOGLE Inc. was sent by post on 28 October 2010 and received on 1 November 2010. A copy of this report was also sent by post to the company GOOGLE France on 28 October 2010 and received on 29 October 2010.

In support of his proposal, the recorder highlighted the discovery of several breaches of the law of 6 January 1978 amended, resulting, in his opinion, from non-compliance with the previously issued formal notice, i.e.:

- Breach of the obligation to complete formalities prior to implementation of the Google Latitude processing operation.
- Violation of privacy and individual liberties.
- Breach of the obligation to collect data in an honest and lawful manner.
- Insufficiency of the responses provided by the company to the Commission's requests.

In addition, the notification letter accompanying the report informed the company that its case was included on the agenda of the restricted committee's meeting to be held on Monday, 6 January 2011 at 2.30 p.m.

The company indicated its written remarks on the report via a letter from its legal advisor, dated 28 December 2010. In addition, it reiterated these remarks in defence, orally, at the meeting of the CNIL restricted committee held on 6 January 2011.

The company, without casting doubt on the accuracy of the acts observed, essentially pleaded the irregularity of the procedures initiated by CNIL, the inapplicability of the law of 6 January 1978, amended in August 2004, to the Google Latitude service, the cessation of all breaches indicated in the formal notice and the goodwill shown by the company in its cooperation with CNIL in this case.

### III. REASONS FOR THE DECISION

#### 1. Concerning the alleged irregularity of the on-site inspection decisions

In its written documents, as during proceedings, the company maintains that the different on-site inspections conducted by CNIL in this case violated the provisions of the law of 6 January 1978 amended.

- First of all, the company reproaches the Commission's services for having proceeded with seven on-site inspections on the basis of a sole and unique decision to proceed with one inspection, in this case, the decision adopted by CNIL's chairman on 17 May 2010. This, according to the company, would be contrary to the "French Data Protection Act."

On this point, the restricted committee finds that no provision of the law of 6 January 1978 amended binds CNIL's chairman to adopt several decisions to conduct several on-site inspections when the inspections conducted all relate to one and the same subject.

In this regard, it notes that the decision of the Commission's chairman, dated 17 May 2010, justifies the conduct of inspections in this case considering that *"it is important to check compliance by the company GOOGLE Inc., represented by the company GOOGLE France, located at 38 avenue de l'Opéra in Paris (75002), with all provisions of the law of 6 January 1978, amended on 6 August 2004."* It also specifies that the on-site inspection mission will take place *"on this company's premises and, if necessary, at any other place involved in the processing operations or files implemented on behalf of the company GOOGLE Inc."* The decision, which intentionally does not specify a particular date for the inspection mission, is drafted in such a way as to allow a possible extension of inspections both in space and in time.

Besides the elements in the file, it emerges that the inspections conducted by CNIL's services with the company GOOGLE France, representing the company GOOGLE Inc., were organised in the continuity of the same proceedings and therefore can not be considered to concern different subjects. For example, it notes that the inspection conducted on 18 January 2010 was agreed upon with the company during the previous inspection on 11 December 2009 to allow the Commission's services to examine a *"Google car"* in working order. Similarly, the purpose of the inspection of 4 June 2010 was to obtain submission of the computer copies mentioned in the formal notice of 26 May 2010, itself referring to inspections conducted by CNIL's services prior to this date.

In view of the previous, it can not be disputed that the purpose of all the inspections conducted in this case was to allow CNIL to obtain perfect understanding of the operation of the geolocalisation services proposed by the company GOOGLE Inc., represented by the company GOOGLE France and establish whether or not the processing operations implemented in this context complied with the "French Data Protection Act."

Consequently, the restricted committee considers that the decision of the Commission's chairman, adopted in May 2010, could legitimately serve as the basis for the succession of inspections conducted in this case.

- Secondly, the company maintains that CNIL's inspectors allegedly did not inform the associates of the company GOOGLE France of the purpose of the inspections conducted *"at the latest, before the start of these inspections"* but during the course of the successive inspections. This, according to the company, would be contrary to the provisions of paragraph 1 of article 62 of the decree of 20 October 2005, which specifies that *"when the*



*Commission conducts an on-site inspection, it informs the site manager of the purpose of the inspections it intends to conduct along with the identity and capacity of the people entrusted with conducting it."*

Concerning this point, the restricted committee finds that the reports, compiled by CNIL's inspectors and signed by the company's representatives after the inspections, show that the company was systematically informed of the purpose of the inspections by CNIL's inspectors before the start of inspections at the latest.

It also notes that the purpose of these inspections was sometimes even communicated well before their execution, either by telephone or by e-mail, as indicated in the inspection reports drafted after these missions, in compliance with the law. For example, the company was informed by e-mail, dated 13 July 2010, of the organisation of an inspection on its premises to be conducted on 21 July 2010, accompanied by a list of very precise, unequivocal questions concerning the purpose of the inspection. Similarly, the company was informed in advance by e-mail, dated 23 July 2010, of the purpose of an inspection scheduled for 30 July 2010 on its premises.

In addition, the restricted committee emphasises that the signatures on the reports drafted after the inspections indicate, all without exception, that the site manager had effectively been informed *"of the purpose of the inspections and the identity and capacity of the people entrusted with conducting them"* and that these documents were signed without any remarks on this point included by the company's representatives.

Consequently, it considers the company's objection to this point irrelevant.

- Thirdly, the company maintains that the on-site inspection procedures implemented by the Commission's services were irregular insofar as they were not the subject of prior, legal authorisation,

Concerning this point, the restricted committee finds that the law in force does not in any way bind CNIL's services to request prior authorisation from the judicial authority for the inspections they conduct. An authorisation request of this nature is only made in a subsidiary manner in the event of the site manager objecting to the conduct of an inspection. In its *Inter Confort* and *Pro Décor* decrees of 6 November 2009, the Council of State effectively considered that *"the right of the site manager to object to the visit [by CNIL], which can only be exercised with the authorisation and under the control of the judicial authority, offers a guarantee equivalent to prior authorisation granted by the judge."* Since the company did not object to the inspections imposed upon it, it can not reasonably plead the irregularity of the procedures conducted by CNIL on these grounds.

## **2. Concerning the alleged irregularity of the formal notice issued**

In its written documents, as during proceedings, the company reproached CNIL for having adopted the formal notice of 26 May 2010 before expiry of the deadlines granted during the inspection of 19 May 2010; it thus considers that the formal notice, adopted less than 5 working days after the inspection of 19 May, was adopted in an irregular manner.

Concerning this point, the restricted committee finds, on examining the elements in the file, that the report on the inspection of 19 May 2010 specified several deadlines according to the requests formulated by the inspection delegation after the said inspection. On reading this report, it appears that a deadline of five working days was specifically granted to the company for submission of the source code for the computer program used up to 14 May

2010, identifying the part of the code that resulted in the collection of data relative to the content of WiFi terminals and the replies to various questions. On the other hand, it turns out that the inspection delegation granted a distinct deadline of three days for the company to provide CNIL with a complete copy *"of the data relative to content from WiFi terminals in France, isolated by Google Inc."*

The deadline for transfer to CNIL of the content of WiFi communications captured in France was therefore effectively three working days. Taking into account the fact that the Commission's premises were closed on 24 May, it results from the previous that the deadline fixed by the inspection delegation expired on 25 May 2010. The formal notice adopted by the Commission's executive committee on 26 May was therefore effectively adopted after expiry of the deadline granted to Google during the inspection of 19 May 2010.

Consequently, the restricted committee can not allow the company's objection on this point.

### **3. Concerning the alleged insufficiency of the deadline granted to the company to respond to the penalty report**

In its written documents, the company considers that it did not have sufficient time or information to respond to the penalty report addressed to it on 28 October 2010.

In this regard, it maintains that, since the formal notice adopted by the restricted committee and the CNIL IT department's expert report were drafted exclusively in French, CNIL violated article 6-3 of the European Convention on Human Rights, which stipulates that *"everyone charged with a criminal offence has the following minimum rights (...) To be informed promptly, in a language he understands and in detail, of the nature and cause of the accusation against him."* Moreover, with the time necessary to translate these documents added to the deadline for response to the formal notice, the deadline for compliance specified by the formal notice adopted in summary proceedings was, in the company's opinion, excessively short (seven days).

Concerning this point, the restricted committee reminds that the very purpose of formal notice addressed urgently is to enjoin the body in question to comply with the law immediately, indicating the breaches observed and the measures to be taken to remedy them. Under such circumstances, the provisions of article 73 of the application decree of the "French Data Protection Act" stipulate that, in an emergency, the executive committee may adopt a compliance deadline shorter than ten days.

In this case, the seven-day deadline granted to the company therefore seems perfectly in line with the applicable legal and regulatory provisions.

It also emerges from the elements in the file that Mr. Philippe GOSSELIN, a CNIL member, was only appointed recorder before the restricted committee on 7 October 2010, i.e. more than four months after adoption of the formal notice. The company therefore had the possibility to remedy the breaches observed within this four-month period preceding the hearing.

The restricted committee therefore considers that, in view of these circumstances, the company is unreasonable in maintaining that it was subject to a hurried procedure with no regard for its rights.



Concerning the difficulties that the company allegedly encountered in satisfying CNIL's requests because the latter did not supply the procedural documents in English, the restricted committee points out that a legal precedent established by the Council of State stipulates that written notification in the French language does not infringe the rights of the body in question so long as the latter is represented by a French lawyer (decree of 7 December 2005, company RYANAIR, no. 270424, published in the Lebon report). Since the company GOOGLE Inc. had a legal advisor in France, such a translation was therefore unnecessary. In addition, the restricted committee points out that CNIL did send the company the penalty report translated into English, which indicates the Commission's will to respect the company's right to a fair trial within the meaning of the European Convention on Human Rights and Fundamental Freedoms.

Consequently, the restricted committee does not allow the objection formulated by the company against CNIL any more than the previous one.

#### **4. Concerning prior characterisation of the collected data as data of a personal nature**

##### Applicable texts

Article 2 of the law of 6 January 1978, amended in August 2004 stipulates that: *"Personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration."*

In addition, article 2 of Directive 95/46 of 24 October 1995 relative to the protection of natural persons with regard to the processing of data of a personal nature and the free flow of this data stipulates that *"is understood to mean (...) a "personal data": any information relating to a natural person who is or can be identified (person in question), directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, psychological, economic, cultural or social identity."*

This definition is completed by Recital 26 of the directive, which stipulates that *"the principles of protection must apply to any information relating to a person who is or can be identified (...) In order to determine whether a person is identifiable, all the means likely to be reasonably implemented, either by the data controller or any other person to identify the said person must be taken into consideration; the principles of protection do not apply to data made anonymous in such a way as to render the person in question no longer identifiable; (...)."*

##### Concerning SSID and MAC data combined with localisation data

The recorder maintains that the SSID and MAC data, combined with the localisation data collected by the "Google car" vehicles, is data of a personal nature, which the company contests, indicating its "doubts" on this point.

In order to rule on the question of characterisation in this case, the restricted committee noted the following elements.

Although it is certain that the scope of the data-protection rules must not be extended excessively, it is nevertheless accepted that the concept of data of a personal nature is defined extensively both by the above-mentioned European Directive 95/46 and by the law of 6 January 1978 amended. Thus, it emerges from the preparatory work on Directive 95/46 that the identification of a person does not necessarily depend on knowing certain proven elements of identity (name, first name, etc.) but may depend on a whole range of other elements (trade, nationality, age, telephone number, working conditions, etc.). This point is expressly raised in opinion 4/2007 delivered by the group known as the "article 29 group," an independent European Union advisory body on the protection of data and privacy, mentioned by the recorder in his report.

Concerning the SSID identifiers, the company indicates that they only rarely contain the names/first names of natural persons, that even supposing that this identifier reveals the use of a name or first name, it would not be possible to identify a particular person because of possible name duplications and finally, it would be difficult to confirm that the person supposedly identified was necessarily the person using the network.

The restricted committee, for its part, notes that the SSID identifiers make it possible to identify the WiFi networks within range and connect to them and that these identifiers frequently contain the name and/or first name of the network owners; such elements therefore obviously make it possible to identify a natural person. This data must be considered as constituting data of a personal nature.

Concerning the MAC addresses, the company maintains that they would only identify a router, not a natural person, that several users could use the same router to access the Internet and that it is conceivable that the MAC address has been usurped by a third party, thus, it is impossible to pre-suppose in a definitive manner that a stable link exists between a MAC address and a natural person.

In this regard, the restricted committee considers that a MAC address, which only identifies the WiFi router that allows users to access the Internet can not be characterised as data of a personal nature on its own. However, a MAC address can be captured by Internet sites during the user's navigation after the latter has identified him/herself. Once linked to these identification elements, it necessarily constitutes data of a personal nature.

It is according to such elements of context that it is necessary to decide whether or not a MAC address may be considered data of a personal nature.

Concerning the question of knowing if this data, combined with localisation data, is likely to be characterised as data of a personal nature, the company maintains that such a combination would not make it any easier to identify natural persons since the localisation data in the company's possession is only approximate. Notwithstanding, it maintains that CNIL's expert report itself would not be able to identify any natural persons from the combination of SSID, MAC and localisation data since, in addition, the precise location of a WiFi router can only be determined accurately in sparsely populated areas.

It also reminds that only the resources likely to be reasonably implemented by the data controller must be taken into account in considering a natural person identifiable, in compliance with recital 26 of the above-mentioned directive 95/46/CE. In its opinion, it would be extremely difficult to locate the precise location of a router and, consequently, to implement the reasonable resources necessary to proceed with the identification of its owner.

On this point, the restricted committee points out that, in this case, the "Google car" vehicles recorded their own GPS coordinates at the same time as the MAC addresses of the WiFi access points for the purpose of collecting localisation data making it possible, *in fine*, to determine the geographic position of users of the *Latitude* service (and, incidentally, of other geolocalisation services proposed by the company GOOGLE Inc. calling upon the "GLS" localisation database). The possibility to locate one, identified natural person therefore constitutes, in its essence and substance, the purpose of the service in question.

Consequently, the restricted committee considers that insofar as this data makes it possible to determine the location of users of the service, it reveals their behaviour with particular acuity within the meaning of the Directive and G29's work. The purpose of collecting MAC addresses, combined with the other information collected, leads the restricted committee to consider that this data, when added together, constitutes data of a personal nature.

This analysis is supported by the fact that it emerges from the report, uncontested on this point at the hearing, that localisation databases such as the "GLS" base allow users not only to search for a person using his/her name or address but also carry out a search using the MAC address of a WiFi router. Entry of the MAC address then makes it possible to obtain the geographic location of the WiFi access point in question.

If it is true that this procedure does not in all cases allow accurate determination of the location of the access point sought, particularly in densely populated areas, it is nevertheless possible, in this hypothesis, to move to the premises indicated by the localisation service on the basis of the transmission power variations of the WiFi router sought. On this point, the restricted committee therefore agrees with the recorder's analysis.

It does not therefore subscribe to the company's argument, according to which the location of a house via collection of MAC addresses would be "*extremely difficult*," since the purpose of this collection is precisely to constitute a localisation database constituting a map of the territory in order to be able to provide a geolocalisation service for users of the *Latitude* service.

It therefore considers, in this case, that the combined collection of SSID identifiers and MAC addresses, in association with geolocalisation data, is of a nature to characterise the collection operation initiated by the company in this case as processing data of a personal nature within the meaning of article 2 of the law of 6 January 1978 amended.

#### Concerning content data

In addition, the recorder maintains that the content data ("*payload data*") collected by the company via the "Google cars" is data of a personal nature.

Conversely, the company maintains that this content data is not data of a personal nature. To this end, it argues that the content data was recorded in binary format, illegible to man, therefore making it impossible to identify natural persons. Moreover, it indicates that it only converted it into legible format after CNIL's request, that no natural person could be formally identified after CNIL's analysis of the data and that the data was essentially fragmented.

On this point, the restricted committee points out the following elements:



First of all, it can not accept that the recording of the data in a format illegible to man would have an impact on their characterisation as data of a personal nature: if not, it would simply be a matter of encrypting initially legible data to escape the provisions of the "French Data Protection Act."

In addition, the restricted committee observes that, as admitted by a company director in the above-mentioned press release of 22 October 2010 and as recorded by the recorder both in his written documents and during the hearing, the company admitted recording complete e-mails, web addresses and passwords by means of its "Google cars" to the point of stating that "*we failed badly*" and "*we are mortified by what happened*" in this case. In such a context it can not therefore agree with the company's argument according to which only fragmented information, escaping as such from characterisation as data of a personal nature, was collected.

On the contrary, it notes that CNIL's services discovered consulted web sites, electronic addresses, their geographic location, identifiers and passwords for personal accounts and the content of electronic mail in the data supplied by the company. This data undisputedly constitutes data of a personal nature within the meaning of the law of 6 January 1978 amended, without it being necessary to determine the names and first names of the people involved to retain this characterisation.

Under these conditions, it therefore considers that the MAC addresses and SSID identifiers, combined with the localisation data collected by the company and, a fortiori, content data, must be considered data of a personal nature, subject, as such, to protection by the "French Data Protection Act."

#### **5. Concerning breach of the obligation to complete formalities prior to implementation of processing operations**

All data controllers are bound by the obligation to complete the prior formalities with CNIL before implementing an automated personal-data processing operation, in compliance with the provisions of chapter IV of the law of 6 January 1978.

Under the terms of formal notice no. 2010-216 of 26 May 2010, the company was accused of a breach of the obligation to complete prior formalities for the following reasons:

- The *Latitude* system was not submitted to CNIL for prior formalities before its implementation.
- In the context of the formalities with CNIL concerning the "*Street View*" system (declaration no. 1303459), the company did not declare the collection of WiFi-router SSID identifiers and MAC addresses and connection data from WiFi terminals.

The Commission's executive committee then enjoined the company to proceed with the declaratory formalities required for the *Latitude* system and, concerning the *Street View* service, cease all collection of WiFi-router SSID identifiers and MAC addresses and connection data from WiFi terminals, since this collection was not declared in a regular fashion.

The restricted committee notes, first of all, that the declaration relative to the *Street View* service was amended to take CNIL's request into account, although "*without prejudice*." It therefore considers that the requirements of the formal notice in this matter were met, albeit indirectly.

However, it notes that the company did not always proceed with the formalities specified in Chapter IV of the above-mentioned law of 6 January 1978 for the *Latitude* system.

The company defends itself on this point, considering that the company GOOGLE Inc., established in the United States, does not have recourse to any processing resources on French territory with which to implement the *Latitude* system for which it is responsible. Implementation of this system would therefore not be subject to French law since the provisions of the "French Data Protection Act" are applicable to data processing operations executed by a controller not established on French territory only insofar as the latter "has recourse to processing resources located on French territory" (article 5-1-para 2).

Even accepting that the company can not be considered "*established on French territory*," which is however debatable because of the establishment of a distinct legal entity in Paris (SARL GOOGLE France), the restricted committee does not subscribe to the restrictive interpretation of the "*processing resources*" concept that the company defends to escape application of the "French Data Protection Act."

This concept can not effectively be reduced to the sole use of equipment or proprietary materials, as the company pretends.

If it is true that the English language version of article 4 of the above-mentioned Directive 95/46, which transposes article 5 of the "French Data Protection Act" into French law, is drafted in a more restrictive manner than the other authentic linguistic versions of the text, it is nevertheless established that the concept of "*equipment*" used in the English version must be subject to wide interpretation, corresponding to that of "*processing resources*" used in both the French version of the text and in its other linguistic versions, in which its literal equivalent is included.

The restricted committee must therefore determine whether processing resources are implemented on French territory in the context of the *Latitude* service.

On this point, it notes, first of all, that it emerges from the company's written documents, confirmed on this point at the hearing, that the *Street View* and *Latitude* services, both accessible via *Google Maps* and, in more general terms, all the geolocalisation services proposed by the company, depend on a common database (the above-mentioned "GLS" base). It is agreed that the "*Google car*" vehicles, which the company recognises as constituting processing resources within the meaning of law, were used as a first-line to constitute the part of this database relative to France, using GPS and radio signals. Implementation of the geolocalisation services proposed by the company in France therefore depends on a database principally constituted by processing resources located in France.

In addition, the restricted committee notes that the *Latitude* service cannot operate without calling upon processing capacities specific to the terminal and known only to it, particularly the GPS chip, when present, if not, the GSM aerial or, as in this case, the WiFi access point. Once this data has been collected by the terminal, on which prior installation of the company's application is necessary, the data is sent to the company's servers (in this case, the "GLS" base, located in the United States) to return the map corresponding to his/her location in France to the user.

It follows therefore that what precedes implementation of the *Latitude* service depends, at least partially, on the recourse to processing resources deployed on French territory, i.e. as much the "*Google car*" vehicles as the users' terminals used for geolocalisation purposes.

This is why the restricted commission considers, contrary to what the company maintains, that the latter implemented processing resources located on national territory and that French law is applicable to the processing operations executed in the context of implementation of the *Latitude* service in France.

Finally, the restricted committee considers that the company can not suggest that CNIL never considered the failure to declare the *Latitude* service a breach before pronouncement of the formal notice of 26 May 2010, since two letters from CNIL's chairman, dated 14 May 2009 and 20 April 2010, reminded the company of the applicability of the law to this service and invited the company to declare *Latitude*.

Under these conditions, it notes that the company did not fulfil its obligation to declare this system on the day of the hearing. It therefore notes that the company did not satisfy the request relative to this matter in the formal notice.

## **6. Concerning respect of privacy and individual liberties**

Article 1 of the law of 6 January 1978 amended stipulates that *"Information technology should be at the service of every citizen. Its development shall take place in the context of international cooperation. It shall not violate human identity, human rights, privacy or individual or public liberties."*

Under the terms of formal notice no. 2010-216 of 26 May 2010, the company was accused of a failure to respect privacy and individual liberties linked to *"the collection, recording and storage by the company GOOGLE Inc. of data from WiFi terminals likely to contain information on Internet sites consulted by the people in question, on the content of messages exchanged and the identifiers and passwords enabling connection to certain sites."*

Consequently the Commission's executive committee enjoined the company to *"cease all collection of data without the knowledge of the people concerned in the context of "Google Street View" processing, particularly concerning WiFi network identifiers (SSID), MAC addresses of WiFi routers and connection data from WiFi terminals."*

In its response to the formal notice, the company confirmed that it had *"ceased all collection of WiFi data using Street View vehicles, as announced publicly in its official blog on 14 May 2010."* It maintains that this breach had ceased by the day of the hearing, before the formal notice had even been issued.

On this point, the restricted committee considers that a commitment made by a company by way of a press release does not prevent CNIL from ensuring compliance with the law, including in a more restrictive manner, by adopting a formal notice. This was all the more justified because the acts of which the company was accused had an international impact at the time and the company had admitted their seriousness in its own statements.

On the substance, neither can the restricted committee retain the argument according to which the people involved did not suffer any violation of their rights and liberties in the absence of any re-use of this data and that, consequently, this breach is not proven.

On the contrary, it considers that this breach is characterised as soon as a considerable quantity of data has been captured without the knowledge of persons over a large part of national territory and that the data is, in its essence and substance, of an extremely personal nature (identifiers, passwords, connection data enabling identification of sites consulted, e-



mail exchanges). In particular, it notes that the data collected reveals, in some cases, the sexual orientation of persons or their state of health, i.e. sensitive data within the meaning of the "French Data Protection Act."

Consequently, the restricted committee considers that there was unlawful collection contrary to article 1 of the law of 6 January 1978 amended and that violations of privacy, secrecy of correspondence and freedom of speech were committed. However, it considers that the commitment made by the company to cease collection, recording and storage of data from WiFi terminals is effectively equivalent to having put an end to the violation.

In addition, although the entirety of the source code of the software called into question, which alone would formally allow CNIL to make sure that the breach reproached had effectively ceased, was not submitted to the Commission, the restricted committee notes that the Commission's services were able to establish that cessation of this collection was effective during the inspection missions conducted with the company.

Consequently, it considers that this count of breach can not be retained as a basis for imposing a penalty on the company.

## **7. Concerning breach of the obligation to collect data in an honest and lawful manner**

Under the terms of paragraph 1 of article 6 of law no. 78-17 of 6 January 1978 amended, data of a personal nature must be collected and processed in an honest and lawful manner.

Under the terms of formal request no. 2010-216 of 26 May 2010, the company was accused of breaching the obligation to carry out an honest and lawful collection of data linked to *"the collection of WiFi network identifiers (SSID), MAC addresses of WiFi routers and connection data from WiFi terminals, [...] collected without the knowledge of the people concerned."* Consequently, the Commission's executive committee enjoined the company to *"ensure that it no longer collected data of a personal nature in a dishonest or unlawful manner in the context of Google Street View processing."*

In its response to the formal notice, the company indicates that *"although it is not established that Google collected personal data in a dishonest or unlawful manner in the context of the Street View service or the collection of WiFi data, [it confirms] that Google has stopped collecting all WiFi data by means of Street View and wishes to continue to cooperate with the authorities in this case."* In addition, the company reminds that it also undertook to cease all collection of WiFi data by means of its *"Google cars."*

Before the restricted committee, the recorder maintains that the WiFi data collected by the *"Google cars,"* including content data, was collected unlawfully because it was without the knowledge of the users concerned, the latter, a fortiori, not having been informed of their rights.

Even though the company indicated that it was no longer collecting this data using *"Google cars"* following the formal notice, the recorder pointed out that it had nevertheless not stopped using the data thus collected for the purpose of providing its geolocalisation services. Proof of this fact is the amendment to the declaration submitted to CNIL relative to the *Street View* service, which includes the addition to the data collected of *"WiFi network identifiers and the MAC addresses of WiFi routers."*

The recorder thus considered that the company did not provide the appropriate elements for establishing the absence of a dishonest and unlawful manner in the collection of WiFi data in the context of the *Street View* service and left, at the very least, a doubt remaining as to its intentions with regard to the MAC addresses and WiFi identifiers already collected.

In its defence, the company maintains that it did not proceed with any dishonest and unlawful collection as far as the collection of content data by the "*Google car*" vehicles is concerned. Certainly, it does admit to an error on this point but maintains that it had never intended to collect the data recorded by these vehicles.

However, it contests having breached its legal obligations with regard to personal information in the collection of MAC addresses and SSID identifiers. In effect, it maintains that it would require a disproportionate effort to supply the information required by law to each of the people concerned (supposing that they are known), which would exonerate it from its obligations in application of article 32-III of the "French Data Protection Act." This article effectively stipulates that "*these provisions (relative to informing people) shall not apply (...) whenever the data subject has already been informed or whenever informing the data subject proves impossible or would involve disproportionate efforts compared with the interests of the procedure.*"

On this point, the restricted committee retains that the company effectively undertook to cease all collection of data from WiFi terminals, secured or not (MAC addresses, SSID identifiers and communication content), using "*Google car*" vehicles and that this undertaking was made prior to the issue of formal notice.

However, it points out that the company's written documents indicate that it will effectively continue to use the MAC addresses and SSID identifiers of the WiFi network users thus collected to provide its geolocalisation services although it is established that they were collected without the knowledge of their owners. In addition, it understands the explanations provided by the company, during the inspections and at the hearing, which indicate that the GLS base will no longer be fed WiFi data by means of the "*Google cars*" but rather by the mobile terminals of the users of its geolocalisation services ("*smartphones*," laptop computers, etc.). It notes that the company is still not informing the owners of the WiFi networks from which they now collect the data by this means.

In the two hypotheses, a lack of information of this nature can not be accepted on principle since this data must be considered of a personal nature within the meaning of the law.

In this regard, the restricted committee accepts that informing the owners of the MAC addresses and WiFi identifiers personally is effectively impossible to implement under such circumstances since no direct link exists between the company and these people, including when the company is collecting their data via the terminals of the users of its geolocalisation services.

That said, it considers that the company can not exempt itself from providing general information on the collection of this data and on the rights of persons in this regard. By way of comparison, it points out that the company implemented numerous general information measures concerning the collection of photographs by the "*Google cars*," either in the local press or by on-line posting of information on the company's .fr Internet site to allow people to object to the distribution of data concerning them, on-line and on the same site.



Consequently, the restricted committee considers that the dishonest and unlawful nature of the collection of data persists, at least in part, and, as a result, constitutes an on-going breach of the terms of the formal notice of 26 May 2010.

#### **8. Concerning the insufficiency of the responses provided to the Commission's requests**

Article 21, paragraph 2 of the law of 6 January amended stipulates that *"the ministers, public authorities, executives of state-owned or private companies, heads of various groupings and more generally the holders and users of data processing and personal data filing systems may not oppose the actions of the commission or its members. They must rather take all useful steps to facilitate its task."*

Under the terms of formal notice no. 2010-216 of 26 May 2010, the company was accused of providing insufficient responses to CNIL's requests, particularly in the context of the inspections conducted in December 2009 and January 2010.

The formal notice thus pointed out that the vehicle presented to the delegation during the inspection of 18 January 2010 *"did not contain a hard disk, preventing any examination of the latter."*

The company was also accused of not having submitted a copy of all data relative to content from WiFi terminals in France to the Commission within the deadlines granted during the on-site inspection conducted on 19 May 2010.

Consequently, the Commission's executive committee enjoins the company to *"submit to the Commission the information and copies requested during the on-site inspection conducted on 19 May 2010, as indicated in the report and, in particular, provide CNIL with a copy on an IT medium of all data collected in France via WiFi terminals in the context of Google Street View" processing.* It also requested that the company prove to CNIL that all the above-mentioned requests were satisfied within the deadlines granted.

The company responded to the formal notice as follows:

First of all, it states that, during the inspection of 4 June 2010, it submitted a copy of the report on the audit conducted at its request by the STROZ FRIEDBERG audit office, a *"copy of the last hard disk sent to the United States containing data from a collection operation conducted by a Street View vehicle in France"* and a copy of the *"data relative to content from WiFi terminals in France, isolated by GOOGLE Inc."*

Secondly, it adds that it submitted the source code of the computer program used in the *Street View* vehicles that enabled collection of content data, reminding that it considered the requests to concern only the software that enabled collection of WiFi data and not the entirety of the software installed in the vehicles.

Thirdly, since this was the source code for the software used on resumption of collection operations, it reminds that it had stopped collecting data relative to WiFi networks by means of *Street View* vehicles. It indicates that it *"will give CNIL a copy of the one or more new software packages implemented, not including WiFi data-collection functions, as soon as these elements become available."*

Notwithstanding, the recorder considers that the company responded to CNIL's requests in an unsatisfactory manner.

He reproaches the latter for particular casualness, if not reticence in informing the Commission, during the inspections conducted by CNIL on 11 December 2009 and 18 January 2010, of the fact that, in addition to the photographs and GPS data, the "Google car" vehicles were also recording MAC addresses and SSID identifiers.

He also points out that the company revealed the recording of content data not by specific letter but by way of a press release, published on 14 May 2010, although CNIL had questioned it three times between December 2009 and February 2010 about the collection carried out.

On the substance, the recorder again reproaches the company for its reticence in submitting the source code implemented in the vehicles to the Commission. In his opinion, the company sought refuge behind a restrictive interpretation of the Commission's requests in order to submit only the source code for the *gSlide* software that enabled collection of the WiFi data, the latter not in any way satisfying the request expressed in the formal notice, which specifically mentioned *"the part of the code that resulted in the collection of data relative to content from WiFi terminals."*

The belated communication of new elements of the source code, by e-mail dated 12 July 2010, does nothing more to satisfy the request expressed in the formal notice; these latter elements did not make it possible to determine the operation of the software serving to collect content data from WiFi terminals since they were limited to the launch code of the WiFi data-collection tool.

According to the recorder, the company therefore abstained from responding to the formal notice and even contented itself with delaying tactics by submitting a report on an audit conducted at its request as the sole element to assist analysis of its collection software.

The company again defended itself on this point both in writing and at the hearing.

It maintains that the vehicle inspected on 18 January 2010 did not contain a hard disk because of a misunderstanding of the CNIL officials' intentions in this matter. It indicates that the presence of WiFi aerials on the roof of the vehicle effectively shows that, at no time, did the company seek to hide from CNIL the fact that it was collecting MAC addresses and SSID identifiers. It maintains that these acts took place prior to the issue of formal notice and, consequently, can not justify the adoption of a financial penalty on the basis of the texts in force.

In addition, concerning the source code that enabled collection of WiFi data, the company contests the fact that the law allows CNIL to request communication of source codes on the basis of its article 44-III: even if the latter stipulates that CNIL's officials can access computer programs and data in the context of inspection missions and request their transcription, it does not, on the other hand, make any reference to software source codes. It is because of its will to cooperate with CNIL that the company, in spite of everything, decided to submit the latter. In addition, the company considers that the part of the source code submitted to CNIL's officials allowed them to proceed with the checks they wished to conduct.

Finally, concerning the source code used after resumption of "Google car" activities, the company maintains that despite the incidents indicated by the recorder, none of them prevented CNIL's officials from noting that the WiFi aerials had been removed from the vehicles and that, consequently, the latter would no longer collect any data from WiFi terminals. Incidentally, the company would not have put its vehicles back on the road without having removed the WiFi-data recording devices.

On this point, the restricted committee retains the following elements:

If the contested collection of WiFi data can be imputed, at the very least, to characterised negligence in preparing a data-collection program as massive as this, all the more open to criticism because it comes from a dominant actor in the market, it does not emerge from the facts of the case that the reactions of the company in face of the requirements formulated by CNIL during the investigation can be characterised in the same way. Consequently, the restricted committee does not retain the term bad faith against the company to characterise its relations with CNIL in this case.

On the other hand, it is established that neither the old nor the new source codes for the collection software were submitted to CNIL since only partial elements of the initial source code and no element of the new source code were submitted.

Concerning the old source code: it is established that analysis of the source code submitted by the company during the inspection of 4 June 2010 revealed that only a fraction of the WiFi data-collection software, corresponding to the recording of GPS positions, was submitted to CNIL. It is also established that analysis of the patch for this software, sent by the company in July 2010, revealed that only part of the source code, corresponding only to the launch of the software, was addressed to CNIL. CNIL therefore had to content itself with the audit office's report, compiled at the request of the company itself, to understand the operation of the "gStumbler" software and, in more general terms, operation of all the software installed in the "Google cars."

Concerning the new source code: the fact that CNIL was able to note the absence of a WiFi key in one of the 22 "Google car" vehicles put back on the road in France is, undoubtedly, an element of a nature to assure it of the sincerity of the company's undertaking to cease collection of WiFi data. Nevertheless, it is no substitute for submission of the source code requested, which alone allowed CNIL to make sure that this collection was impossible in all the vehicles on the road. CNIL's expectations in this matter are all the more legitimate since the company had undertaken to "give a copy of the one or more new software packages implemented, not including WiFi data-collection functions, as soon as these elements become available" - and this, well before issue of the formal notice adopted by the executive committee on 26 May 2010. The vehicles are currently being driven on the territory and yet this was not the case.

In addition and quite obviously, the restricted committee can not subscribe to the company's restrictive reading of article 44 of the law of 6 January 1978 to evade submission of these source codes. The provisions of this article effectively stipulate that CNIL's officials can obtain communication and copies of "*all documents necessary for the performance of their mission, whatever their medium*" during inspection missions. The "document" concept must be widely extended to allow CNIL to execute its missions. In this case, the concept must be extended to cover the source codes of the software from which the collection of WiFi data originated.

Thus, the failure to submit these source codes is the basis for the recorder reproaching the company for not cooperating with the Commission in the context of the inspection missions conducted with the company GOOGLE France, thus placing the company in contradiction with the requirements subsequently imposed by the formal notice.



## 9. Concerning the benefits gained by the breaches committed by the company GOOGLE Inc.

It is a fact that the company gained substantial benefits from the collection of MAC addresses and SSIDs in this case, the latter acknowledging the fact in its written documents.

In effect, the collection of this data, particularly users' MAC addresses, allowed the company to enrich its localisation databases using the MAC addresses of WiFi routers recorded by its moving "Google cars." The data collected gave the company an undeniable advantage over its competitors, allowing it to propose high-performance geolocalisation services. The geolocalisation services proposed by the company, which generate very heavy traffic, are, as a direct result, likely to generate advertising resources, which constitute most of the company's turnover.

In effect, the *Google Maps* service, which includes the *Street View* and *Latitude* services, makes it possible to conduct searches for services or businesses near the position of the geolocalised user. The results displayed in return include, in particular, commercial links paid for by Google Inc.'s advertisers. A link to the *Google* search engine is also included in *Google Street View*.

The collection of tens of thousands of WiFi access points by means of the "Google cars" has allowed the company to constitute a significant geolocalisation database and, consequently, to acquire a dominant position in the geolocalisation services sector.

Apart from this undeniable advantage, the company also benefits from the fact that it is no longer necessary for it to collect new WiFi data itself to ensure that the GLS base remains operational. In effect, on connecting, the users' terminals detect not only the access points included in the base but also, depending on the case, new access points located close by or those that have disappeared: this information is then recorded automatically by the company for the purpose of enriching and updating the GLS base. As a result, the collection of WiFi data by the "Google cars" is effectively no longer necessary since the collection of data transmitted automatically by the users' terminals is now sufficient to ensure the continuity of the mobile geolocalisation services proposed by the company.

The company has thus acquired a new technique giving it an undeniable competitive advantage. It obviously gains an economic advantage from this situation because it can propose new geolocalisation services to its users that will themselves generate an audience and, consequently, new advertising revenues.

In addition, considering that processing of the data thus collected on French territory is not governed by the law of 6 January 1978 amended, the company exempted itself from the legal obligations incumbent upon it, particularly those concerning completing prior formalities with CNIL and informing people. This situation has continued since the launch of the *Street View* service in France, i.e. since February 2009.

The company also gained an organisational advantage from the observed breaches with the absence of appropriate measures taken to ensure the legal certainty of the *Street View* project upstream and compliance with the right of persons to object downstream. In addition, these breaches must be related to the extreme sensitivity of the project, to its ambition to cover the entire French territory and to the significance of the resources available to the company.

The company therefore gained considerable benefits from the breaches it committed in this case.

#### **10. Concerning the breaches observed**

Consequently, in view of the persistence of certain breaches mentioned in the formal notice issued by the restricted committee on 26 May 2010, a financial penalty amounting to €100,000 (one hundred thousand Euros) will be imposed on the company GOOGLE INC.

#### **11. Concerning publication of the decision**

In view of the nature and seriousness of the breaches committed and, on the one hand, the necessity for natural persons to know the rules relative to protection of their personal data and, on the other, for data controllers to better understand the rules imposed upon them, the Commission's decision will be published on CNIL's Internet site and on the Légifrance Internet site.

However, this decision will not be the subject of a press insertion in the absence of bad faith, established within the meaning of article 46 of the law of 6 January 1978 amended.

### **ON THESE GROUNDS**

In compliance with section I of article 45 of the law of 6 January 1978 amended, CNIL's restricted committee, after due deliberation, decides to:

- Impose a financial penalty of €100,000 (one hundred thousand Euros) on the company GOOGLE INC.
- Announce this decision publicly on CNIL's Internet site and on the Légifrance Internet site.

The company GOOGLE INC. has a period of two months starting on the date of notification of this decision within which to lodge an appeal against it before the Council of State.

Paris, 17 MARCH 2011

The Chairman  
Alex TÜRK

# CNIL

The General Secretary

GOOGLE FRANCE  
The Manager  
38 avenue de l'Opéra  
75002 PARIS

## LETTER DELIVERED TO ADDRESSEE IN PERSON

*References to quote in all correspondence:*  
CTX-2010-050

Paris, 18 March 2011

Dear Sir,

Please find enclosed a copy of CNIL's decision no. 2011-035, addressed today by letter to the company GOOGLE INC.

Should you require any further information, please contact Ms. Elise WOLTON, head of the sanctions department (33 (0)1 53 73 25 44 / 25 37).

Yours faithfully,

Yann PADOVA

Enclosure: copy of decision no. 2011-035



**Lampert, O'Connor & Johnston, P.C.**

1776 K Street NW, Suite 700  
Washington, DC 20006

E. Ashton Johnston  
johnston@lojlaw.com

tel (202) 887-6230  
fax (202) 887-6231

September 19, 2011

*By Hand Delivery*

Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**  
**File No. EB-10-IH-4055**

Dear Ms. Dortch:

Google Inc. ("Google"), pursuant to Sections 0.457 and 0.459 of the Commission's rules, 47 C.F.R. §§ 0.457, 0.459, hereby requests confidential treatment of the enclosed document. The enclosed material, identified as Document 11-21, falls within Exemption 4 of the Freedom of Information Act ("FOIA"), which provides a statutory basis for withholding from public inspection "matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential."<sup>1</sup>

Specifically, Document 11-21 contains detailed, specific information regarding Google's private business and internal operations. The Document consists of a translation which was paid for and obtained by Google as the result of a request by the Enforcement Bureau in connection with the above-referenced matter. The document "would customarily be guarded from competitors," *see* 47 C.F.R. § 0.457(d)(2); Google has not made this document available to the public or to any third parties,<sup>2</sup> and voluntarily provides it at this time with the assumption that it will be treated confidentially. Confidential treatment is warranted in this case because the Internet service industry in which Google operates is highly competitive, and the Document and the information it contains relate to Google's business and operations. *See* 47 C.F.R. § 0.459(a)(4).

---

<sup>1</sup> 5 U.S.C. § 552(b)(4).

<sup>2</sup> *See Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 975 F.2d 871, 879 (D.C. Cir. 1992) (holding that commercial information provided on a voluntary basis "is 'confidential' for the purpose of Exemption 4 if it is of a kind that would customarily not be released to the public by the person from whom it was obtained.").



**Lampert, O'Connor & Johnston, P.C.**

Request for Confidential Treatment - File No. EB-10-IH-4055

September 19, 2011

Page 2

We enclose herewith both a complete, unredacted copy of this submission, to be treated as confidential, and a separate copy marked REDACTED. Consistent with 47 C.F.R. § 0.459(d)(1), Google requests notification by the Commission if release of the redacted material in the Letter is requested pursuant to the FOIA or otherwise, so that Google may have an opportunity to oppose grant of any such request.

Respectfully submitted,



E. Ashton Johnston  
Joseph A. Bissonnette  
*Counsel to Google Inc.*

Enclosure

cc: Theresa Z. Cavanaugh, Acting Chief, Investigations and Hearings Division, Enforcement Bureau (by email)  
Mindy Littell, Investigations and Hearings Division, Enforcement Bureau (by email)

**Michael Rubin**  
Direct Dial: (650) 849-3311  
[mrubin@wsgr.com](mailto:mrubin@wsgr.com)

June 15, 2012

*Via Federal Express*

Michael Morisy  
MuckRock News  
DEPT MR 1314  
PO Box 55819  
Boston, MA 02205-5819

**Re: Google FCC Documents**

Dear Mr. Morisy:

Please see the enclosed documents.

Sincerely,

WILSON SONSINI GOODRICH & ROSATI  
Professional Corporation

/s/  
Michael Rubin

Enclosures

Google Inc.  
Public Policy Department  
1101 New York Avenue, NW  
Second Floor  
Washington, DC 20005



Phone 202.346.1100  
Fax 202.346.1101  
www.google.com

December 10, 2010

**CONFIDENTIAL TREATMENT REQUESTED**

***Via Hand Delivery***

Marlene H. Dortch  
Secretary, Federal Communications Commission  
236 Massachusetts Avenue, N.E., Suite 110  
Washington, D.C. 20002

Attn: Mindy Littell  
Investigations and Hearings Division  
Enforcement Bureau  
Federal Communications Commission  
445 12th Street, S.W., Room 4-C330  
Washington, D.C. 20554

Re: **Google Inc., File No. EB-10-IH-4055**

Dear Ms. Littell:

This letter is the response of Google Inc. ("Google") to the letter dated November 3, 2010 ("Letter") from P. Michelle Ellison, Chief, Enforcement Bureau, Federal Communications Commission ("Bureau"), which requests information about Google's collection of data from Wi-Fi networks in the United States.

The Letter initiates an investigation into whether Google's actions violated Section 705 of the Communications Act, as amended, 47 U.S.C. § 605 ("Section 605"). As will be shown, Google's data collection in the United States involved the passive reception of publicly broadcast Wi-Fi information, and Google has not disclosed that data to any person and has not used that data in any product or service, nor has such data been used for the benefit of any person or entity in any way. Consequently, Google did not violate Section 605.

As background and for some context on this issue, it may also be helpful to describe the basic information that is publicly broadcast by Wi-Fi networks. A Wi-Fi network is configured to permit enabled devices (such as a laptop or mobile phone) to find wireless access points and to connect to the Internet. To do so, the network broadcasts a radio signal with its “service set identifier,” or SSID, and its unique hardware or router identifier, known as a MAC address, in addition to other network-related information. This broadcast information can be detected by Wi-Fi-enabled devices to facilitate the network connection. The network owner can choose to make the network openly accessible (not encrypted and thus accessible by any user’s device) or closed (encrypted and available only to authorized devices).

Google Street View cars were fitted with commercially-available Wi-Fi antennas and software to collect SSIDs and MAC addresses and other network information, which when combined with the GPS location of the cars collecting the data, help improve our location-based services. We variously refer to this non-content information as Wi-Fi network information or simply Wi-Fi information. Wi-Fi information does not and was not used to identify any specific individual or household.

In addition, we had mistakenly included code in our software that collected payload data (information sent over the network) from unencrypted Wi-Fi networks. Google has acknowledged that the unencrypted payload data might contain communications, including URLs, emails or other personal information, but Google has not performed a detailed analysis of the payload data itself, nor has it used it in any product or service.

As soon as we became aware of this collection, we grounded our Street View cars and secured the payload data on our network. We then removed the payload data from the Google network so that it is inaccessible to anyone other than those responsible for securing the data, and we continue to safeguard it.

Google has acknowledged publicly and promptly upon discovering this collection activity that it was a mistake, and apologized for it. It is important to underscore what did not happen:

- No payload data transferred over **encrypted** networks was collected by Google.
- No payload data has been **used** in any product or service by Google.
- No U.S. payload data has been disclosed in any way to third parties.
- The Wi-Fi network data collected contains no personally identifiable information; and
- There has been **no public disclosure or breach** relating to payload information.

Maintaining people's trust is crucial to everything we do and, by mistakenly collecting payload data, we fell short. We appreciate your interest in this matter and would be happy to discuss these issues with you further. We look forward to working with the Bureau to resolve its concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "V. A. Swartz". The signature is fluid and cursive, with the first letters of each name being capitalized and prominent.

Enclosures

cc: Hillary DeNigro (via hand delivery and electronic mail)  
Mindy Littell (via electronic mail)



**CONFIDENTIAL AND PROPRIETARY**  
**File No. EB-10-IH-4055**

**DOCUMENT 11-1**

REDACTED

## GStumbler

Status: *Current* (as of 2007-08-23)

Modified: Thu Aug 23 2007

### Contents

[Objective](#)[Background](#)[Privacy Considerations](#)

## Objective

We will gather Wi-Fi data as part of the Cityblock project's [data acquisition](#). This data will be gathered just once and will be analyzed offline for use in other initiatives. The project is complete when all cityblock vehicles are equipped with Wi-Fi scanning equipment and have completed their work.

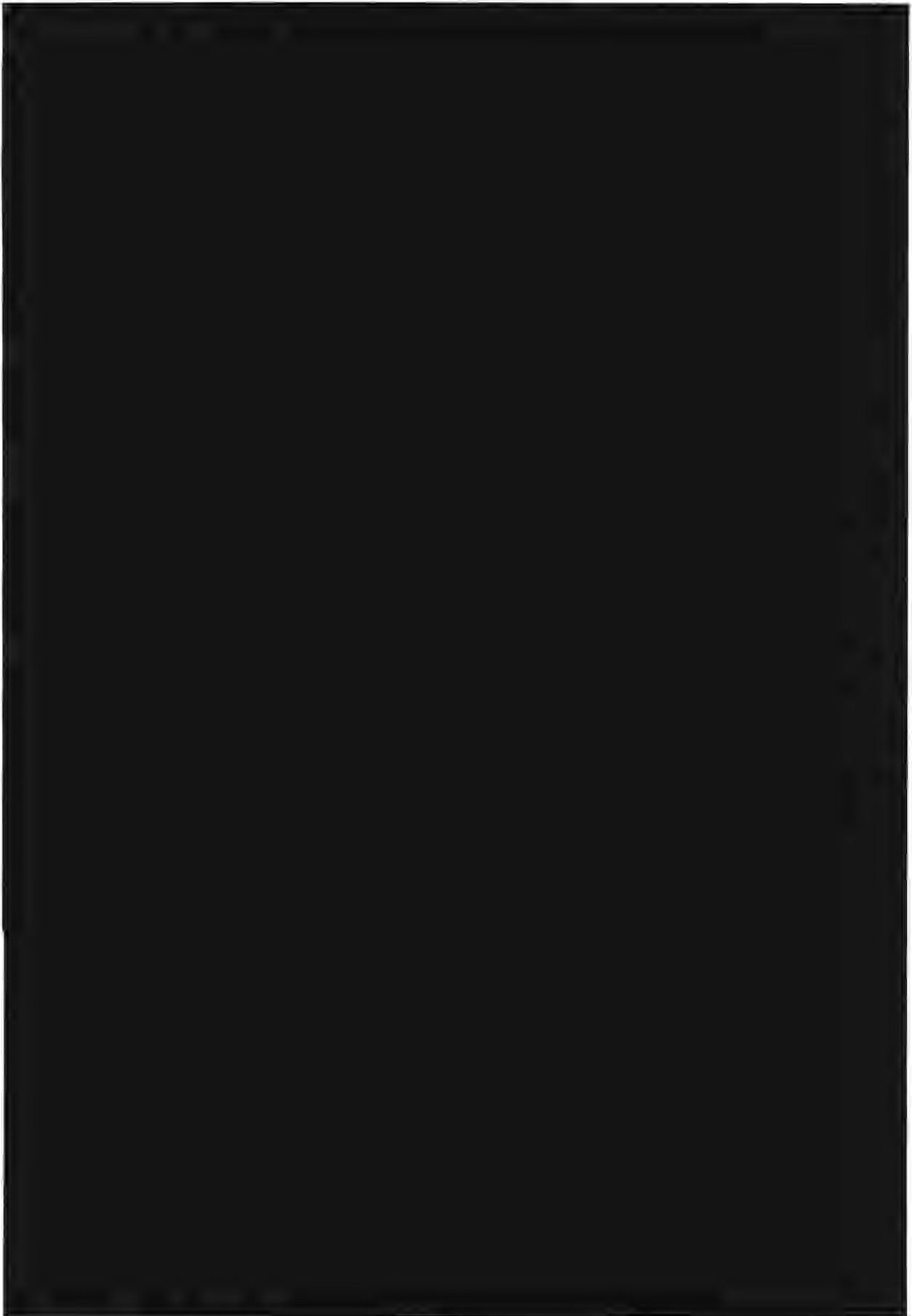
Analysis of the gathered data is a nongoal (though it will happen).

## Background

Data from Wardriving can be used a number of ways. The following is by no means exhaustive:

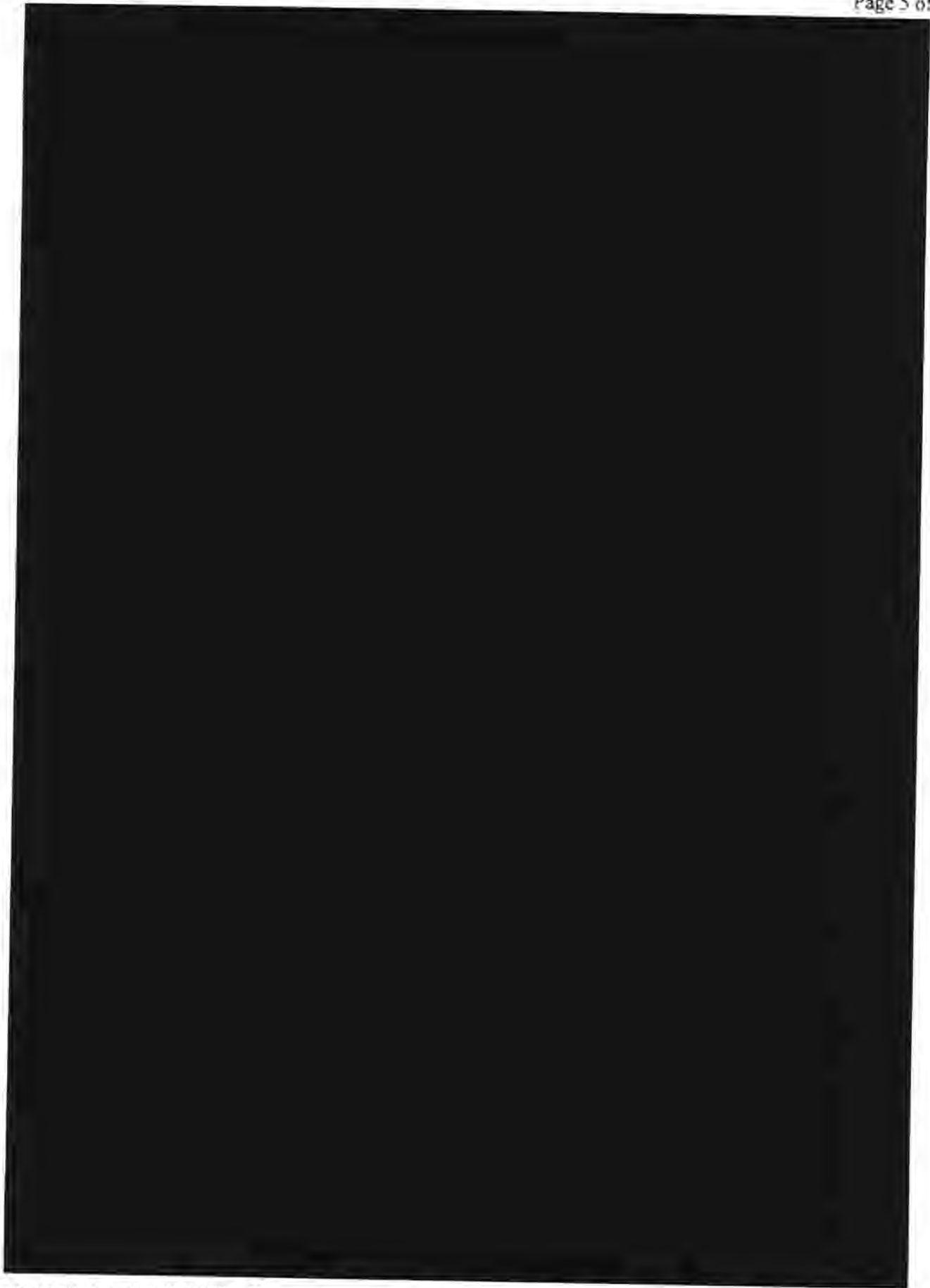
- to provide geolocation of Wi-Fi enabled users
- to determine market penetration of Wi-Fi
- to determine where Wi-Fi access is lacking
- to observe typical Wi-Fi usage snapshots













## Privacy Considerations

[\[Link\]](#)

The gathering of Wi-Fi data has a number of superficial privacy implications. A typical concern might be that we are logging user traffic along with sufficient data to precisely triangulate their position at a given time, along with information about what they were doing. In reality this information is of little use, since the cityblock vehicle is not in proximity to any given user for an extended period of time.

None of the data gathered by GStumbler will be presented to end users of our services in raw form.

*TODO: discuss privacy considerations with [Poulton Kimmel](#).*































































```
12: #include "base/commandlineflags.h"
```







```
128: int main(int argc, char** argv) {  
129:     InitGoogle(argv[0], &argc, &argv, true);
```






























































































```
14: DEFINE_bool(discard_encrypted_body, true,  
15:             "Discard bodies of encrpyted 802.11 frames");  
16: DEFINE_bool(discard_control_frame, false,  
17:             "Discard 802.11 control frames");  
18: DEFINE_bool(discard_data_frame, false,  
19:             "Discard all 802.11 data frames");  
20: DEFINE_bool(discard_management_frame, false,  
21:             "Discard all 802.11 management frames");
```










```
121: // Discard data we don't care about
122: bool TruncateParserImpl::Parse(Dot11Frame *f) {
123:     if (FLAGS_discard_encrypted_body && PacketUtil::IsEncrypted(f)) {
124:         // Discard just the body of encrypted frames
125:         f->clear_body();
126:     }
```



```
128:     switch (PacketUtil::Type(f)) {
129:     case Dot11FrameBody::CONTROL:
130:         if (FLAGS_discard_control_frame)
131:             f->set_discard(true);
132:         break;
133:     case Dot11FrameBody::DATA:
134:         if (FLAGS_discard_data_frame)
135:             f->set_discard(true);
136:         break;
137:     case Dot11FrameBody::MANAGEMENT:
138:         if (FLAGS_discard_management_frame)
139:             f->set_discard(true);
140:         break;
141:     default:
142:         break;
143:     }
```

